UNIVERSIDAD NACIONAL DE INGENIERÍA

RECINTO UNIVERSITARIO PEDRO ARAUZ PALACIOS

FACULTAD DE CIENCIAS Y SISTEMAS

TRABAJO MONOGRÁFICO PARA OPTAR AL TÍTULO DE INGENIERO DE SISTEMAS

TÍTULO:

"Propuesta de contextualización de mecanismos, normas y procedimientos para la realización de una auditoría de sistema al módulo de caja de una institución financiera de primer piso en Nicaragua."

AUTOR:

- ✓ Br. Leonel Enrique Canda Soza. 2002-14196
- ✓ Br. Rene Antonio Flores Centeno. 2003-19023

TUTOR:

MSC. Ing. Eveling Espinoza Aragon.

Miércoles, 11 de diciembre de 2017

Managua, Nicaragua

Dedicatoria

Dedico este trabajo a mis padres que me inculcaron desde pequeño el amor al trabajo, a esforzarme y seguir adelante a pesar de las vicisitudes, a mis tres (3) hijos que son un verdadero regalo a mi vida. También dedico este trabajo a mis amigos que me ayudaron para seguir adelante, a mis maestros que sirvieron en el transcurso del camino del aprendizaje siendo un baluarte en mi vida, a los maestros en el trabajo que he tenido y que también son una bendición de Dios. E importante para mí, indicar que esta dedicaría va para mi Dios, porque sé y siento que él ha puesto su mano en todo momento – Amén.

Leonel Canda Soza

Dedico este trabajo monográfico a mis hijas, regalo del Señor. A mis dos hijos que están en el Cielo. A mi esposa, por su amor y su apoyo. A mis padres, que han luchado para darme lo mejor. A mis hermanos mayores, que son un gran ejemplo para mí. A mi comunidad, hermanos en la fe, que me han acompañado durante tantos años en la Iglesia. A Dios, que le ha dado sentido a mi vida y que me regala este momento de culminación de estudios...

René Flores Centeno

Resumen

El presente trabajo de investigación monográfico está dirigido a proponer una guía metodológica para la realización de auditoría de sistemas para el módulo de caja de un banco de primer piso, contextualizando las mejores prácticas para la realización de auditoría de sistemas.

Para lograr nuestro objetivo desarrollamos una investigación no experimental - documental del tipo informativa, dado que no requerimos realizar una manipulación deliberada de las variables ni tampoco definirlas sino que deseamos conocer las prácticas actuales de los auditores internos al momento de realizar auditorías de sistemas en las instituciones bancarias de primer piso, para evidenciar que ciertamente sí existen políticas y procedimientos internos para realizar este tipo de auditorías pero que son de uso y conocimiento exclusivo de la institución y, por lo tanto, consideramos necesario proponer una contextualización de las mejores prácticas para aportar y exponer información primaria a esta área de conocimiento de tal forma que sea de fácil acceso y comprensión para el público interesado en desarrollarse profesionalmente en la realización de auditorías de sistemas.

Con esta investigación pretendemos contribuir a la comunidad universitaria y a los profesionales dedicados a roles asociados a informática así como a auditores internos en general brindando mayor información documental sobre el desarrollo de una auditoría de sistemas, especialmente a instituciones bancarias de primer piso.

ÍNDICE

I. INTRODUCCION

El Sistema Financiero de Nicaragua está conformado por un conjunto de instituciones, que intermedian recursos o servicios financieros con la función principal de canalizar el ahorro que generan los clientes o unidades con superávit, hacia los prestatarios o con déficit (Intermediación).

Las Instituciones Financieras bancarias forman parte de este sistema y según la Ley 516 – Ley General de Bancos - son los autorizados para realizar las operaciones de intermediación con recursos obtenidos del público en forma de depósitos o a cualquier otro título, y/o a prestar otro tipo de servicios financieros, todo esto conocido como operaciones pasivas y activas. Cabe destacar que los bancos son regulados por la Superintendencia de Bancos y Otras Instituciones Financieras (SIBOIF).[1]

Una gran cantidad de estas operaciones de intermediación financiera se registran y controlan a través del módulo de caja que cada banco diseñó de acuerdo a sus necesidades y capacidades tecnológicas, entre estas tenemos: depósitos a cuenta (con efectivo o cheque), retiro de efectivo, pago de servicios públicos (agua, luz, teléfono, etc.), y otro tipo de servicios como el pago de préstamos, compra y venta de divisas (mesa de cambio), pago de multa entre otros.

Las Instituciones Financieras requieren implementar una serie de controles sobre los sistemas informáticos que soportan los procesos relacionados a su funcionamiento. Estos controles deben ayudar a asegurar la integridad, confiabilidad y disponibilidad

[1] La SIBOIF es el ente regulador de las instituciones financiera (bancos de primer piso establecidos en Nicaragua), entre ellos tenemos: Banco de la Producción, S.A. (BANPRO), Banco de América Central (BAC), Banco la FISE (BACENTRO), Banco Avanz, Ficohsa, Banco de Finanzas (BDF).

de los datos, así como evaluar si las aplicaciones cumplen con los lineamientos regulatorios y si apoyan al cumplimiento de los objetivos de la organización.

Partiendo de lo anterior, nuestro trabajo consiste en proponer un mecanismo en el que se contextualice los Marcos de Referencia y las Mejores Prácticas sobre la implementación de una auditoría de sistemas de tal forma que sirva de material de referencia a una área de auditoría de sistemas de la Unidad de auditoría interna y así mismo a las personas que se interesen en desarrollar esta profesión.

II. ANTECEDENTES

A partir de un proceso de investigación que hemos realizado en bibliotecas de universidades nacionales y en el Repositorio Universitario de Nicaragua perteneciente al Consejo Nacional de Universidades (CNU) observamos información limitada sobre guías didácticas que cuenten con ejemplos claros sobre cómo realizar una auditoría a los sistemas de información y en correspondencia a nuestro tema, a la realización de una auditoría a un módulo de un sistema en particular, a como es el módulo de caja de un banco de primer piso.

Partiendo de lo anterior, encontramos dos investigaciones relacionadas que complementan nuestro tema de investigación a como son: 1) *Propuesta de Manual de Procedimiento de Auditoría Informática en el Ministerio de Transporte e infraestructura (MTI),* de la Universidad Politécnica de Nicaragua (UPOLI) y 2) La Tesis titulada *Propuesta Guía Metodológica para ejecutar Auditorías Integradas* de la Universidad Nacional de Ingeniería (UNI).

En la primera investigación se observa cómo la Lic. Jazmina Molinares realiza una propuesta para el Ministerio de Transporte e Infraestructura (MTI) en donde, implementando normas de control interno emitidos por la Contraloría General de la República y aplicando estándares internacionales como ISO27002 y marcos de trabajo COBIT, desarrolla un manual de procedimientos que sea aplicable para una Institución Estatal (Molinares, 2014). En esta propuesta logramos observar y analizar que dicho manual de procedimientos puede ser considerado como una fuente de información primaria para nuestra investigación, pero el enfoque utilizado por la Lic. Molinares está orientado a cumplir con los requerimientos de auditoría para el sector estatal de Nicaragua.

En la segunda investigación, el Ing. Davis Porras, el cual es un Auditor de Sistemas de Información Certificado (CISA) propone desde un enfoque holístico cómo desarrollar Auditorías Integradas en la que las diferentes disciplinas de auditoría se interrelacionan para realizar de manera efectiva el control de riesgos y procesos claves dentro de una organización (Rodríguez, 2014). Esta investigación del Ing. Porras fue una fuente primaria de información para nuestra propuesta metodológica debido a que cubre el área de conocimiento que deseamos contextualizar, pero su alcance incluye la aplicación holística de un único enfoque para las distintas disciplinas involucradas en el proceso de auditoría interna. En cambio, el alcance de nuestra metodología está delimitado a la realización de auditoría interna de sistemas para el sector financiero, específicamente para el área de caja de una institución financiera de primer piso en Nicaragua.

III. JUSTIFICACION

Dada la confidencialidad de la información interna de las Instituciones Financieras en Nicaragua, sobre todo en sus procesos de auditoría, observamos - a partir de una revisión previa - que hay muy poco material que sirva como guía metodológica para la realización de auditorías informáticas en este tipo de instituciones.

Se cuenta con una vasta cantidad de información primaria (libros, normas técnicas emitidas por instituciones reguladoras, entre otros) pero en nuestro contexto nacional, para el sector bancario, no existe una propuesta metodológica que esté directamente orientado a la auditoría de sistemas para el Core Bancario, específicamente dirigido a una auditoría al módulo de caja de una institución bancaria de primer piso.

En consecuencia, propondremos una serie de procedimientos para el desarrollo de una auditoría de sistemas al módulo de caja de una institución financiera con el fin de demostrar con base en la recopilación de mejores prácticas y experiencia, las herramientas y procedimientos que se deben ejecutar en cada fase de la auditoría a como son Planeación, Ejecución, Presentación de Resultados y Seguimiento a Oportunidades de Mejora[2].

El desarrollo de este trabajo monográfico espera también beneficiar a los estudiantes de la carrera de ciencias en computación y sistemas que aspiren a desarrollarse en el mercado laboral de Nicaragua, específicamente “Auditoria de Sistemas Informática”, con lineamientos o ejemplos de herramientas claras de cómo

[2] Las fases aquí mencionadas son las que se exponen en la metodología propuesta.

desarrollar una auditoría de este tipo, tomando como referencia la consolidación de conocimientos y mejores prácticas como COBIT, ITIL, ISACA (CISA) y las NIA.[3]

[3] **COBIT**: Objetivos de Control para Información y Tecnologías Relacionadas/ **ITIL**: La Biblioteca de Infraestructura de Tecnologías de Información/ **ISACA**: Asociación de Auditoría y Control de Sistemas de Información/ **CISA**: Certified Information Systems Auditor. NIA: Normas Internacionales de auditoría.

IV. OBJETIVOS

Objetivo General

Proponer una guía metodológica para el desarrollo de una auditoría de sistema al módulo de caja de un banco de primer piso en Nicaragua.

Objetivos Específicos

- Proponer una auditoría de sistema para el módulo de caja considerando las etapas de planeación, ejecución, presentación de resultados y seguimiento a las oportunidades de mejoras.

- Proponer y estandarizar una serie de instrumentos que faciliten al auditor llevar un control sobre los procedimientos realizados en cada fase de la auditoria.

- Ejemplificar el proceso de planeación, ejecución, presentación de resultados y seguimiento a las oportunidades de mejora a través de una auditoría al módulo de caja.

V. MARCO TEORICO

A continuación presentamos una serie de elementos teóricos relacionados a nuestro tema de estudio con los cuales pretendemos facilitar una perspectiva conceptual del contexto de nuestra investigación.

Sistemas

Sistema

Conjunto de elementos, todo unitario y organizado compuesto por dos o más partes relacionadas de modo dinámico, que desarrollan una actividad para alcanzar determinado objetivo o propósito. Requiere de materia, energía o información obtenida del ambiente que constituyen los insumos o entradas (inputs) de recursos necesarios para que el sistema pueda operar. Estos son procesados en las diversas partes del sistema (subsistema) y transformados en salidas o resultados (ouputs) que retornan al ambiente.[4]

Sistema de información (SI)

Es un conjunto de elementos que interactúan con el fin de apoyar las actividades de una empresa o negocio.[5] Los elementos formarán parte de alguna de las siguientes categorías: Personas, Datos, Actividades o técnicas de trabajo, Recursos materiales en general (generalmente recursos informáticos y de comunicación). Todos estos elementos interactúan para procesar los datos (incluidos los procesos manuales y automáticos) y dan lugar a información más elaborada, que se distribuye de la

[4] Cris Edwars & John Word, Sistema de información. P.24.

[5] Cohen Karen, Daniel y Asin Lares, Enrique. Sistemas de información para los negocios: Un enfoque para la toma de decisiones. P.6.

manera más adecuada posible en una determinada organización, en función de sus objetivos estratégicos.[6]

Características del sistema

Para alcanzar los objetivos por los cuales fueron diseñados, los sistemas interaccionan con su medio ambiente, formado por todos los objetos que se encuentran fuera de las fronteras, los mismos interactúan con su medio ambiente (reciben entradas y dan salidas). A esto se le conoce como sistemas abiertos, en contraste con aquellos que no interactúan con su medio ambiente (sistemas cerrados), en la actualidad generalmente todos los sistemas son abiertos.[7]

Ambiente de Sistema

Es todo lo que rodea a un sistema y sirve para proporcionarle los recursos necesarios para su existencia. Todo sistema existe y funciona en un ambiente al cual le entrega sus resultados. En este sentido, el ambiente está constituido por factores económicos, tecnológicos, sociales, políticos, legales, culturales, demográficos, entre otros.

Estos ejercen una serie de efectos que inyecta complejidad al macro ambiente en el cual funcionan las empresas. Por otra parte, también existen factores cercanos a las organizaciones como son los proveedores, clientes, competidores, organismos reguladores, etc. quienes imponen restricciones, condiciones y limitaciones al quehacer organizacional.[8]

[6] Cohen Karen, Daniel y Asin Lares, Enrique. Sistemas de información para los negocios: Un enfoque para la toma de decisiones. P.7.

[7] James A. Senn, Análisis y Diseño de Sistemas de Información. P.21.
[8] Cris Edwars & Hohn Word, S.I, P.32

Soluciones de Core Bancario:

La plataforma donde se combinan la tecnología de la comunicación y la tecnología de la información, para satisfacer necesidades básicas de la banca, se conoce como Soluciones de Core Bancario.[9]

Las instituciones bancarias centralizan sus operaciones en su Core bancario, esto quiere decir que la información se procesa en tiempo real. Por ejemplo, un cliente puede realizar un depósito de efectivo en su cuenta de ahorro en una sucursal y hacer retiro de efectivo de esa misma cuenta en cualquier otra sucursal, en un ATM o hacer uso del dinero de su cuenta para realizar transacciones en la banca electrónica.

Sistema de servicio al cliente – Área de Caja

Los servicios financieros que se ofrecen a los clientes o gestores (front office), específicamente en las áreas de caja a través de las distintas sucursales o ventanillas a nivel nacional, abarcan una serie de procedimientos manuales y automáticos que juntos funcionan como un solo sistema de servicio.

Estos servicios funcionan como un intercambio de divisa entre el cliente o gestor y el banco, es decir, la captación (débitos) y entrega (créditos) de dinero que se efectúan durante un lapso de tiempo determinado, dejando como evidencia y/o soporte para el banco el registro de las operaciones a través de los sistemas y para los clientes, la entrega de un comprobante físico o voucher[10].

A manera general entre los servicios principales que se ofrecen tenemos: a) Cambios de cheques, b) Mesas de Cambios, c) Pagos de servicios básicos, d) Pagos de Tarjetas, e) Depósitos a cuentas en efectivo o con cheque, e) Retiros de Cuentas

[9] Core Bancario, (s.f.) Wikipedia. https://es.wikipedia.org/wiki/Core_bancario
[10] **Voucher**: Recibo o constancia de pago que sirve para comprobar que se ha pagado un producto o servicio.

utilizando tarjetas de débito/crédito o con libreta de ahorro, f) Pago de Préstamos, entre otros.

Institución financiera de primer piso

Son instituciones que legalmente están autorizadas para realizar operaciones de ahorro, financieras, hipotecarias y de capitalización. Tienen relación directa con los clientes.[11]

En Nicaragua, los bancos de primer piso son BAC (Banco de America Central), BANPRO (Banco de la Producción), Banco LAFISE Bancentro, BDF (Banco de Finanzas), Banco Ficohsa y Banco Avanz.

Gestión de Riesgo Empresarial

El Marco Gestión de Riesgo Empresarial - Un enfoque integral (Enterprise Risk Management; ERM, según sus siglas en inglés) emitido por el "Committee of Sponsoring Organizations of the Treadway Commission (COSO)", es un marco de referencia utilizado por el Instituto de Auditores Internos como una de las mejores prácticas aplicables en el ejercicio profesional de Auditoria.

Por consiguiente, el presente trabajo monográfico ha como se indicó anteriormente, se centra desde la perspectiva de Auditoría Interna por lo que se hace imperativo conocer los siguientes términos:

Gobierno Corporativo

El Gobierno Corporativo es un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan

[11] https://www.eco-finanzas.com/diccionario/B/BANCOS_DE_PRIMER_PISO.htm, recuperado el 08 de noviembre de 2018.

afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos.[12]

Riesgo

Existen muchas definiciones de riesgo, lo que quiere decir que tiene distintos significados para diferentes personas. Tal vez una de las definiciones de riesgo más sucintas usadas en el negocio de la seguridad de la información es la provista por las Directrices para la Gestión de Seguridad de TI, publicadas por la Organización Internacional de Estandarización (ISO): "El potencial de que una amenaza determinada explote las vulnerabilidades de un activo (G.3) o grupo de activos y, por consiguiente, ocasiones pérdida o daño a la organización".[13]

También un concepto general de riesgo se conoce como la posibilidad de que se produzca un evento que tendrá un impacto en el logro de los objetivos estratégicos de la empresa. El riesgo se mide en términos de impacto y probabilidad.

Evaluación de Riesgos

Los controles de TI se seleccionan e implementan en función de los riesgos para cuya gestión están diseñados. A medida que se identifican los riesgos, se determinan las respuestas adecuadas y estas abarcan desde no hacer nada y aceptar el riesgo como un coste del negocio, hasta la aplicación de un amplio rango de controles específicos, incluyendo la contratación de seguros.

Las evaluaciones de riesgos deben identificar, cuantificar y priorizar los riesgos contra criterios para aceptación del riesgo y objetivos relevantes para la organización. Los resultados deben guiar y determinar la acción apropiada de la

[12] **COSO-ERM:** Conceptos Generales, V 2004.

[13] Manual de preparación CISA, 22ª Edición, sección 1.4. P.49

gerencia y las prioridades para gestionar los riesgos de seguridad de la información y para implementar controles seleccionados para proteger contra estos riesgos.

El alcance de una evaluación de riesgo puede ser o bien toda la organización, parte de la organización, un sistema de información individual, componentes específicos del sistema, o servicios en los que esto es practicable, realista y útil.[14]

3.1 Riesgo inherente:

Se conoce como el valor máximo de los riesgos asociados a un proceso; es decir sin la aplicación de controles

3.2 Riesgo residual:

Se conoce como el valor residual de los riesgos asociados a un proceso una vez que se aplican los controles.

3.3 Riesgo de auditoría:

Es el riesgo de emitir una opinión de auditoria sobre la efectividad y/o suficiencia de los controles.

Control

Todas las acciones tomadas por la dirección, el consejo de administración y demás partes para gestionar el riesgo y favorecer el logro de los objetivos y metas establecidas. La dirección planifica, organiza y dirige la realización de acciones suficientes para brindar una seguridad razonable de que se lograrán los objetivos y las metas.

Dentro del tema de control, a como se ha mencionado anteriormente, existe un marco de referencia generalmente utilizado por las empresas, el Modelo COSO

[14] Manual de preparación CISA 22ª, Capítulo I, Sección 1.6.7. P.58

(Committee of Sponsoring Organizations), el cual se encarga de dictar los elementos básicos para establecer un adecuado sistema de control interno.

Evaluación de los controles:

Los controles de TI no existen en forma aislada. Forman una continuidad interdependiente de protección, pero también pueden estar sujetos a una situación comprometida debido a un enlace débil. Están sujetos a errores y a invalidaciones de gestión, pueden abarcar desde simples hasta altamente tecnificados y pueden existir en un entorno dinámico.

Los controles incluyen políticas, procedimientos y prácticas (tareas y actividades) que son establecidos por la gerencia para proveer una certeza razonable de que se alcanzaran objetivos específicos.[15]

Entendimiento de los Controles TI

Los controles de TI proporcionan aseguramiento relacionado con la fiabilidad de la información y de los servicios de información. Los controles de TI ayudan a mitigar los riesgos asociados con el uso de la tecnología en una organización.

Estos abarcan desde políticas corporativas hasta su implementación física dentro de instrucciones codificadas y desde la protección de acceso físico, a través del seguimiento de acciones y transacciones, hasta las responsabilidades individuales y desde ediciones automáticas hasta análisis de razonabilidad para grandes conjuntos de datos.

Objetivo de Control

Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implementar procedimientos de control en una actividad de TI en particular.[16]

[15] Manual de preparación CISA, 22ª, Sección 1.5, P.52

Los objetivos de control interno se aplican a todas las áreas, ya sean manuales, automatizadas, o bien una combinación de las mismas (es decir, revisiones de registros (logs)). Por lo tanto, conceptualmente, los objetivos de control en un ambiente de SI permanecen sin cambios respecto de los de un ambiente Manual. Sin embargo, la manera como se implementan estos controles pudiera ser diferente. Por lo tanto, los objetivos de control interno se deben tratar de forma relevante para los procesos específicos relacionados con SI.[17]

Los objetivos de control de SI pueden incluir: Salvaguarda de los Activos, asegurar la integridad de los ambientes de sistemas operativos en general incluyendo operaciones de la red, asegurar la identificación y autenticación de los usuarios, cumplimiento con los requerimientos de los usuarios, aseguramiento de la disponibilidad de los servicios de TI, desarrollando planes de continuidad del negocio (BCP) y de recuperación de desastre (DRP).

Controles de Negocio y Controles de TI

El sistema empresarial de controles internos impacta a TI en tres niveles[18]:

Al nivel de dirección ejecutiva, se fijan los objetivos de negocio, se establecen políticas y se toman decisiones de cómo aplicar y administrar los recursos empresariales para ejecutar la estrategia de la compañía. El enfoque genérico hacia el gobierno y el control se establece por parte del consejo y se comunica a todo lo largo de la empresa. El ambiente de control de TI es guiado por este conjunto de objetivos y políticas de alto nivel.

[16] COBIT 4.0, Marco de Trabajo Cobit, P.16, sección Controles

[17] Manual preparación Cisa 22ª, Sección 1.5.2, P.51

[18] COBIT 4.0, Marco de Trabajo Cobit, Idem, P.17

Al nivel de procesos de negocio, se aplican controles para actividades específicas del negocio. La mayoría de los procesos de negocio están automatizados e integrados con los sistemas aplicativos de TI, dando como resultado que muchos de los controles a este nivel estén automatizados. Estos se conocen como controles de las aplicaciones. Sin embargo, algunos controles dentro del proceso de negocios permanecen como procedimientos manuales, como la autorización de transacciones, la separación de funciones y las conciliaciones manuales.

Para soportar los procesos de negocio, TI proporciona servicios, por lo general de forma compartida por varios procesos de negocio, así como procesos operacionales y de desarrollo de TI que se proporcionan a toda la empresa, y mucha de la infraestructura de TI provee un servicio común (es decir, redes, bases de datos, sistemas operativos y almacenamiento).

Los controles aplicados a todas las actividades de servicio de TI se conocen como controles generales de TI. La operación formal de estos controles generales es necesaria para que dé confiabilidad a los controles en aplicación.

Clasificación de los controles

Mediante las definiciones indicadas en el Ítem 6, los controles se pueden clasificar para ayudar a entender sus propósitos y ver dónde se integran dentro del sistema global de controles internos, una clasificación común de los controles de TI es controles generales versus controles de aplicación.

Controles Generales

Los controles generales (también conocidos como controles de infraestructura) se aplican a todos los componentes de sistemas, procesos y datos para una determinada organización o entorno de sistemas.

Los controles generales incluyen, entre otros:

Políticas de seguridad de información,
Administración, acceso y autenticación,
Separación de funciones claves de TI,
Gestión de la adquisición e implementación de sistemas,
Gestión de cambios,
Respaldo,
Recuperación y continuidad del negocio.[19]

Controles Aplicativos

Los controles de aplicación están relacionados con el ámbito de los procesos individuales de negocio o sistemas de aplicación. Incluyen controles tales:
Como ediciones de datos,
Separación de funciones del negocio (ej. la iniciación de transacciones versus autorización),
Cuadre de totales de procesos,
Registro de transacciones e informes de error.

La función de un control es altamente relevante para la evaluación de su diseño y efectividad.

Controles basados en aplicación

El objetivo de los controles internos sobre los sistemas de aplicación es asegurar lo siguiente: a) Todos los datos de entrada son exactos, completos, autorizados y correctos. b) Todos los datos se procesan según lo previsto. c) Todos los datos almacenados son exactos y completos. d) Toda la salida de datos es exacta y

[19] Manual de preparación CISA, Sección 1.5.4, P.42

completa. e) Se mantiene un registro de actividad para rastrear el proceso de los datos desde su entrada, almacenamiento y eventual salida.

En resumen y a manera de ejemplo los controles de aplicación incluidos en los procesos de negocios[20] son:
Integridad
Precisión
Validez
Autorización
Segregación de funciones.

Los controles de aplicación representan un porcentaje importante de los controles de negocio, deben ser la prioridad de cada auditor de TI y necesitan poder evaluar un proceso del negocio, entender y evaluar los controles proporcionados por los procesos automatizados. Dentro de los tipos de controles genéricos que se espera se puedan revisar en cualquier aplicación tenemos los siguientes:

Controles de entrada. Estos controles se utilizan principalmente para chequear la integridad de los datos ingresados dentro de una aplicación de negocio, independientemente de si el dato de origen es ingresado directamente por el personal, remotamente por un socio del negocio o a través de una aplicación Web habilitada. La entrada se chequea para verificar que se encuentre dentro de los parámetros especificados.

Controles de proceso. Estos controles proporcionan un medio automatizado para asegurar que el proceso sea completo, exacto y autorizado.

[20] COBIT 4.0, Marco de trabajo Cobit, P.18, párrafo 1.

Controles de salida. Estos controles se centran en qué se hace con los datos. Deben comparar los resultados con el resultado previsto y verificarlos contra la entrada.

Controles de integridad. Estos controles supervisan los datos de un proceso y/o del almacenamiento para asegurar que los datos siguen siendo consistentes y correctos.

Pista de gestión. Los controles del historial del proceso, a menudo se denominan pista de auditoría y permiten a la dirección rastrear las transacciones desde su origen hasta el último resultado, y viceversa, desde los resultados hasta identificar las transacciones y eventos registrados. Estos controles deben ser adecuados para supervisar la efectividad de todos los controles e identificar los errores tan cerca de sus orígenes como sea posible.
Adicionalmente se debe saber que los elementos universalmente aceptados de seguridad de la información son[21]:

Confidencialidad. La información confidencial debe solamente divulgarse cuando sea adecuado y debe ser protegida contra la revelación no autorizada o interceptación. La confidencialidad incluye consideraciones de privacidad.

Integridad. La integridad de la información se refiere a que los datos deben ser correctos y completos. Esto incluye específicamente la fiabilidad del proceso y los informes financieros.

Disponibilidad. La información debe estar disponible para el negocio, sus clientes y los socios en el momento, el lugar y de la manera más apropiada. La disponibilidad incluye la capacidad de recuperar los servicios de TI ante pérdidas, interrupciones o

[21] ISO 27001:2013 C.4.2

corrupción de datos, así como ante la ocurrencia de un desastre mayor en el lugar donde la información haya estado localizada.

Auditoria

La auditoría es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado, que puede ser una persona, organización, sistema, proceso, proyecto o producto, aunque hay muchos tipos de auditoría, podemos indicar la aplicación de Auditorías Externas e Internas y Gubernamentales.

La actividad de Auditoría Interna: un departamento, división, equipo de consultores, u otros participantes, que proporcionan servicios independientes y objetivos de aseguramiento y consulta, concebidos para agregar valor y mejorar las operaciones de una organización.[22]

Auditoría Externa

Es una auditoría realizada por un profesional experto en contabilidad, de los libros y registros contables de una entidad, para opinar sobre la razonabilidad de la información contenida en ellos y sobre el cumplimiento de las normas contables.

Auditoría Interna

La auditoría interna es un proceso cuya responsabilidad parte de la Alta Gerencia de las compañías y se encuentra diseñado para proporcionar una seguridad razonable

[22] International Standars for th profesional practice of internal auditing. IIA, P.21. Revised October 2012.

sobre el logro de los objetivos de la organización.[23] Estos objetivos han sido clasificados en:

Establecimiento de estrategias para toda la empresa
Efectividad y eficiencia de las operaciones
Confiabilidad de la información financiera
Cumplimiento con las leyes, reglamentos, normas y políticas

La función de auditoría interna ha cambiado notablemente en los últimos años, pasando de una auditoría tradicional orientada a la protección de la empresa (activos) hacia una auditoría enfocada al control de los riesgos, a fin de aumentar el valor de la organización para los accionistas.

Auditoria de Sistemas.

La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.[24] Deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los

[23] International Standars for th profesional practice of internal auditing. IIA, P.04 N1000. Revised October 2012.

[24] Manual de preparación Cisa, 22ª, P.54

sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

ISACA (Information Systems Audit and Control Association)

ISACA comenzó en 1967, cuando un pequeño grupo de personas con trabajos similares—auditar controles en los sistemas computacionales que se estaban haciendo cada vez más críticos para las operaciones de sus respectivas organizaciones—se sentaron a discutir la necesidad de tener una fuente centralizada de información y guías en dicho campo.

En 1969, el grupo se formalizó, incorporándose bajo el nombre de EDP Auditors Association (Asociación de Auditores de Procesamiento Electrónico de Datos). En 1976 la asociación formó una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor en el campo de gobierno y control de TI. Conocida previamente como la Information Systems Audit and Control Association (Asociación de Auditoría y Control en Sistemas de Información), ISACA ahora es solo un acrónimo, que refleja la amplia gama de profesionales en gobierno de TI a los que sirve.[25]

Cuenta con más de 130,000 miembros en más de 188 países. Los beneficios ofrecidos a través de sus investigaciones, certificaciones y colaboración comunitaria globalmente aceptadas dan como resultado una mayor confianza y un mayor valor en los sistemas de información. A través de más de 200 capítulos establecidos en más de 80 países, ISACA brinda a sus miembros educación, intercambio de recursos, abogacía, redes profesionales y una serie de otros beneficios a nivel local.

[25] http://www.isaca.org/about-isaca/history/espanol/pages/default.aspx, recuperado el 08 de septiembre de 2017.

ISACA ofrece las siguientes certificaciones:

Certified Information Systems Auditor (CISA).

Es una certificación para auditores respaldada por la Asociación. Los candidatos deben cumplir con los requisitos establecidos por ISACA.

Certified Information Security Manager (CISM).

Es una certificación para administradores de seguridad de la información respaldada por ISACA. A diferencia de otras certificaciones de seguridad, CISM define los principales estándares de competencias y desarrollo profesionales que un director de seguridad de la información debe poseer, competencias necesarias para dirigir, diseñar, revisar y asesorar un programa de seguridad de la información.

Certified in the Governance of Enterprise IT (CGEIT).

Tiene como objetivo reconocer a una gama de profesionales por su conocimiento y aplicación de los principios de gobierno de TI. Una certificación CGEIT permite a los profesionales ser reconocidos por sus habilidades para comprender el complejo tema de gobernanza de las competencias técnicas, infraestructura de TI y procesos de negocio, y comprender y relacionarse con la gerencia ejecutiva para alinear las TI con la promoción de las metas y objetivos empresariales.

Certified in Risk and Information Systems Control (CRISC).

Esta certificación identifica a los profesionales de TI que son responsables de administrar los riesgos empresariales y de TI. Está dirigido a profesionales de TI encargados de garantizar que se cumplan los objetivos de gestión de riesgos. Un CRISC a menudo está muy involucrado en la supervisión del desarrollo, implementación y mantenimiento de los controles del sistema de información diseñados para proteger los sistemas y administrar los riesgos.

Los miembros de esta organización son los encargados de mantener el framework COBIT. También son los creadores del ITGI (IT Governance Institute) y del marco de trabajo ITAF (Information Technology Assurance Framework).

COBIT (Control Objectives for Information and related Technology)

Los Objetivos de Control para Información y Tecnologías Relacionadas (COBIT por sus siglas en inglés) son una guía de mejores prácticas presentada como marco de trabajo dirigida al control y supervisión de Tecnología de la Información. A Continuación se describen los **Principios de Cobit.**

Satisfacer las necesidades de las partes interesadas[26]**:**

El primer principio se ocupa de la necesidad de alinear las metas individuales, objetivos y prioridades de cada área con la empresa y necesidades de las partes interesadas. Para las empresas es un reto lograr y mantener el alineamiento de los objetivos y necesidades de cada área con los objetivos de la organización, dado que estos objetivos pueden ser cambiantes.

Cubrir la organización de forma integral[27]**:**

El segundo principio reconoce que es crítica la necesidad de que los responsables de las distintas áreas de negocio asuman la responsabilidad de gestionar eficazmente el uso de TI, para permitir que la organización logre cumplir sus objetivos satisfactoriamente.

Aplicar un único marco integrado[28]:

Cobit 5 proporciona un marco general único que constituye una fuente coherente e integrada de orientación en un lenguaje común no tecnológico y agnóstico de la tecnología. Esta fuente puede ser utilizada efectivamente como base de orientación

[26] ISACA (2014).Cobit 5 principles: Where did they come from? [White paper]. P.5
[27] ISACA (2014).Cobit 5 principles: Where did they come from? [White paper]. P.6
[28] ISACA (2014).Cobit 5 principles: Where did they come from? [White paper]. P.8

sobre aspectos específicos sobre la gestión de TI, incluida seguridad de la información, ciberseguridad, riesgo, garantía, gestión de proveedores, gestión de la configuración, control de la nube, etc. de manera efectiva.

ISACA ha hecho una importante inversión a lo largo de los años para que los procesos de COBIT estén alineados con otros estándares y marcos de trabajo, por mencionar algunos como ISO/IEC 38500:2008 (Corporate Governance of Information Technology), ISO/IEC 27001:20138 (Information technology-Security techniques-Information security management systems-Requirements), ISO 9001:200811 (Quality management systems-Requirements), IT Infrastructure Library (ITIL® V3).

Habilitar un enfoque holístico[29]:

La implementación efectiva y eficiente del Gobierno Corporativo de TI requiere un enfoque holístico que toma en cuenta varios componentes denominados "habilitadores" que interactúan entre ellos para apoyar la gestión de la empresa y que son interdependientes.

Para lograr este enfoque holístico con COBIT, se definieron 7 categorías para los habilitadores, los cuales son:

Principios, políticas y marcos de trabajo:

Son los vehículos para traducir el comportamiento deseado en una orientación práctica para la administración diaria.

Procesos:

[29] ISACA (2012).Cobit 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la empresa. P.27

Describen una serie organizada de prácticas y actividades para lograr determinados objetivos y producir una serie de resultados como apoyo al logro de las metas globales relacionadas con TI.

Estructuras Organizacionales: Constituyen las entidades claves para la toma de decisiones en una organización.

Cultura, ética y comportamiento: De los individuos así como de la organización; se subestima frecuentemente como factor de éxito en las actividades de gobierno y administración.

Información: Se encuentra presente en todo el ambiente de cualquier organización; o sea se trata de toda la información producida y usada por la Organización. La información es requerida para mantener la organización andando y bien gobernada, pero a nivel operativo, la información frecuentemente es el producto clave de la organización en si.

Servicios, infraestructura y aplicaciones: Incluyen la infraestructura, la tecnología y las aplicaciones que proporcionan servicios y procesamiento de tecnología de la información a la organización.

Personas, habilidades y competencias: Están vinculadas con las personas y son requeridas para completar exitosamente todas las actividades y para tomar las decisiones correctas, así como para llevar a cabo las acciones correctivas.

Separar el Gobierno de la Administración[30]:

[30] ISACA (2012).Cobit 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la empresa. P.31

COBIT 5 plasma una distinción clara entre el Gobierno y la Administración, dado que comprenden distintos tipos de actividades, requieren distintas estructuras organizacionales y cumplen diferentes objetivos. El Gobierno es responsabilidad de la Junta Directiva bajo el liderazgo de su Presidente y la Administración es responsabilidad de la Gerencia Ejecutiva, bajo el liderazgo del Gerente General.

ITAF (Information Technology Assurance Framework)

ITAF[31] es un modelo de referencia integral y de buenas prácticas que establece lo siguiente:

Establece estándares que abordan las funciones y responsabilidades profesionales de auditoría y aseguramiento de SI; conocimientos y habilidades; y diligencia, conducta y requisitos de informes.
Define términos y conceptos específicos para la garantía de los SI.
Proporciona orientación y herramientas y técnicas sobre la planificación, el diseño, la conducta y el informe de las asignaciones de auditoría y aseguramiento de SI

ITAF, como marco de trabajo, aplica para las personas que ejercen como profesionales de aseguramiento de TI y que se dedican a proporcionar seguridad sobre algunos componentes de sistemas de TI, aplicaciones e infraestructura. Estos estándares fueron diseñados por ISACA de una manera que pueda ser útil para un público más amplio, como por ejemplo a los usuarios de los informes de auditoría y aseguramiento de TI.

IIA (The Institute of Internal Auditors)

[31] ISACA (2017), recuperado el 29 de octubre de 2017 de https://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/Pages/default.aspx

El Instituto de Auditores Internos (IIA por sus siglas en inglés) fue establecido en 1941. Es un órgano de orientación interna para la gestión de riesgos y la auditoría interna. Sirviendo a 185,000 miembros en casi 190 países, el IIA es la organización profesional más grande de auditoría interna con sede central en Estados Unidos. Esta organización ofrece la certificación CIA (Certified Internal Auditor) la cual es reconocida a nivel mundial para los auditores internos y es un estándar mediante el cual las personas pueden demostrar su competencia y profesionalismo en el campo de la auditoría interna.

El Instituto de Auditores Internos ofrece una serie de guías prácticas llamadas GTAGs (Global Technology Audit Guide).

Las GTAG

Las GTAG están escritas en un lenguaje empresarial sencillo para abordar un problema puntual relacionado con la administración, el control y la seguridad de la tecnología de la información (TI). También estas guías ayudan a los auditores internos en todo el mundo a comprender mejor los diferentes problemas de gobernabilidad, riesgos y controles relacionados a la tecnología.

ITIL

La Biblioteca de Infraestructura de Tecnologías de Información es un conjunto de conceptos y buenas prácticas usadas para facilitar que los servicios de TI estén alineados con las necesidades del negocio y que apoyen sus procesos centrales. Permite a las organizaciones e individuos conocer cómo pueden aprovechar la Tecnología de la Información como una herramienta que facilite el cambio, la transformación y el crecimiento del negocio. Está principalmente centrada en la gestión de los servicios de tecnologías de la información[32].

[32] Wikipedia. (30 de 04 de 2017).

Ciclo de Vida del Servicio propuesto por ITIL - 5 fases:

Estrategia del Servicio:

En esta fase se define cuál será la estrategia para satisfacer las necesidades de los clientes, tomando en cuenta los requerimientos de éstos así como los recursos con los que cuenta la organización de TI y considerando qué capacidades deben desarrollarse para cumplir con estas necesidades

Diseño del Servicio:

Su objetivo es diseñar nuevos servicios de TI. Esto puede incluir tanto la creación de nuevos servicios así como la mejora de servicios existentes.

Transición del Servicio:

Su objetivo es crear e implementar servicios de TI. Esta fase asegura que los cambios en los servicios y procesos de TI se lleven a cabo de una manera coordinada y controlada.

Operación del Servicio:

Su objetivo es asegurar que los servicios de TI sean entregados de manera efectiva y eficiente. Incluye el cumplimiento de las solicitudes de los usuarios, la resolución de los fallos del servicio, la solución de problemas y la realización de tareas operativas de rutina.

Mejora continua del Servicio:

Tiene como objetivo mejorar continuamente la eficacia y eficiencia de los procesos y servicios de TI, aprendiendo de los éxitos y fracasos pasados.

ISO/IEC 38500:2008

Proporciona principios rectores para los directores de organizaciones (incluidos propietarios, miembros del consejo, directores, socios, altos ejecutivos o similares) sobre el uso eficaz, eficiente y aceptable de la tecnología de la información (TI) dentro de sus organizaciones. Se aplica al gobierno de los procesos de gestión (y decisiones) relacionados con los servicios de información y comunicación utilizados por una organización.

Estos procesos podrían ser controlados por especialistas de TI dentro de la organización o proveedores de servicios externos, o por unidades de negocios dentro de la organización.

También proporciona orientación a aquellos que asesoran, informan o ayudan a los directores.[33]. El modelo ofrecido por la ISO/IEC 38500:2008 indica que la dirección de la empresa ha de gobernar las TIC mediante tres tareas principales:

Evaluar

Examinar y juzgar el uso actual y futuro de las TIC, incluyendo estrategias, propuestas y acuerdos de aprovisionamiento (internos y externos).

Dirigir

Dirigir la preparación y ejecución de los planes y políticas, asignando las responsabilidades al efecto. Asegurar la correcta transición de los proyectos a la producción, considerando los impactos en la operación, el negocio y la infraestructura. Impulsar una cultura de buen gobierno de TIC en la organización.

Monitorizar

Mediante sistemas de medición, vigilar el rendimiento de la TIC, asegurando que se ajusta a lo planificado.

[33] Iso.org. (2017).Recuperado el 30 de Octubre, 2017 de https://www.iso.org/standard/51639.html

Normas Internacionales de Auditoría (NIA)

La Federación Internacional de Contadores (IFAC por sus siglas en inglés) fue fundada en 1977. Es una organización que aglutina a contadores públicos de todo el mundo para proteger el interés público a través de la exigencia de altas prácticas de calidad.

Esta Organización IFAC creó un comité llamado IAASB (International Auditing and Assurance Standards Board) con el fin de uniformar las prácticas de auditoría y servicios relacionados a través de la emisión de pronunciamientos en una variedad de funciones de auditoría y aseguramiento.

Este comité (IAASB) emite las Normas Internacionales de Auditoría (NIA) utilizado para reportar acerca de la confiabilidad de la información preparada bajo normas de contabilidad. También emite Estándares Internacionales para trabajos de aseguramiento (SAE), Control de Calidad (ISQC) y servicios relacionados (ISRS).[34]

Las NIAs están numeradas de la siguiente manera:

200-299: Principios Generales y Responsabilidad

300-499: Evaluación de Riesgo y Respuesta a los Riesgos Evaluados

500-599: Evidencia de Auditoria

600-699: Uso del trabajo de otros

700-799: Conclusiones y dictamen de auditoria

800-899: Áreas especializadas

[34] Recuperado de https://www.auditool.org/blog/auditoria-externa/1094-nias-normas-internacionales-de-auditoria-y-aseguramiento, 06 Octubre de 2017

VI. DISEÑO METODOLÓGICO

Descripción del diseño de la investigación

Dado que nuestro tema de investigación se refiere a la contextualización de las normas y procedimientos para la realización de una auditoría de sistemas al módulo de caja de una institución bancaria de primer piso en Nicaragua, consideramos que la metodología a aplicar es la de una investigación no experimental, dado que no requerimos realizar una manipulación deliberada de variables ni tampoco definirlas (Sampieri, 2014), sino que deseamos conocer en su contexto natural los procedimientos y las prácticas actuales de los auditores informáticos y personal de TI de estas instituciones bancarias al momento de tener que realizar una auditoría de sistemas al módulo de caja.

Por lo anterior, emplearemos un enfoque no experimental transversal, ya que nos enfocaremos en evaluar una situación o fenómeno en un punto del tiempo, es decir que, a partir de los datos obtenidos del personal de Auditoría Interna y personal de TI de instituciones bancarias (datos que obtendremos con instrumentos específicos) junto con la información documental analizada obtendremos las averiguaciones necesarias para poder proponer una guía metodológica para el desarrollo de una auditoría de sistemas, al módulo de caja de un banco de primer piso.

Descripción del tipo de investigación

Para lograr los objetivos que hemos planteado se realizará una investigación no experimental – documental, del tipo informativa. Según (Sampieri, 2014)" Los estudios exploratorios se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes."

Los procedimientos con los que se realiza una auditoría de sistema en una institución bancaria de primer piso no son de acceso público, por lo tanto, la propuesta que realizaremos pretende aportar conocimientos en esta disciplina tropicalizando las mejores prácticas y estándares existentes de manera sencilla y que a su vez permitan ser replicadas para otras soluciones o módulos informáticos del Core Bancario. Según (Paz, 2014) "La investigación documental es la búsqueda de una respuesta específica a partir de la indagación en documentos".

Para nuestro caso, realizaremos una recopilación adecuada de información que permita organizar las ideas y pensamientos expuestos por los distintos marcos de trabajo y asociaciones que han aportado conocimiento al área de estudio de auditoría de sistemas de tal forma que en base a esta información obtengamos los fundamentos necesarios para proponer la metodología que se presentará como resultado de la revisión de la información recopilada.

Población

Para nuestro tema monográfico, la población está conformada por auditores informáticos que correspondan a la unidad de Auditoría Interna así como jefes y coordinadores del área de informática de las instituciones bancarias de primer piso.

La selección de la muestra se realizará de una manera no probabilística intencional. Se requerirá la opinión de expertos e información de casos tipo, dado que el enfoque de nuestra investigación es exploratorio. Según (Sampieri, 2014) "se utiliza una muestra de casos tipo en estudios cuantitativos exploratorios y en investigaciones de tipo cualitativo, en el que el objetivo es la riqueza, profundidad y calidad de la información, no la cantidad ni la estandarización." Por la naturaleza de nuestra investigación, la información de los participantes y el nombre de la institución financiera se tratarán con confidencialidad.

Descripción de las fuentes de información

1. Fuentes Primarias

- Entrevistas y/o encuestas con personal que tiene experiencia en el desarrollo de auditoría de sistemas de información

2. Fuentes Secundarias

- Publicaciones realizadas por ISACA

- Estándares y marcos de trabajo COBIT, ITIL, COSO, ITAF, NIA

Información requerida a las fuentes

Información general y didáctica sobre el desarrollo de una auditoria de sistemas de información.

Instrumentos para la recolección de información

Entrevistas, elaboración de matrices de riesgo, check List.

Procedimientos para la recolección y elaboración de la información

Entrevistas: Contactar personalmente, por teléfono o por correo electrónico a los entrevistados.

Procesamiento de la información.

El procesamiento de la información se realizará con el apoyo de herramientas de Ofimática.

I. Revisión bibliográfica

Para nuestro tema de investigación realizamos una revisión de varios documentos relacionados a los estándares, mejores prácticas y marcos de trabajo sobre la realización de auditorías.

En el siguiente cuadro indicamos los documentos de mayor relevancia analizados para realizar nuestra propuesta metodológica:

Autor	Año	Título	Aportes
Committee of Sponsoring Organizations of the Treadway Commission	2016	Enterprise Risk Management - Aligning Risk with Strategy and Performance	Análisis de Riesgo, Marco de trabajo para Gestión del Riesgo.
The Institute of Internal Auditors IIA	2012	Global Technology Audit Guide (GTAG®) 1 Information Technology Risk and Controls	Explicación de la importancia de los controles de TI y del entendimiento del ambiente de TI en general, desde un enfoque de análisis del riesgo.
International Federation of Accountants (IFAC)	2012	International Standards on Auditing (ISA) - Normas Internacionales de Auditoría (NIA)	Explica un conjunto de prácticas y estándares para la realización de auditorías internas.
The Institute of Internal Auditors IIA	2012	International Standards for the Professional Practice of Internal Auditing	Detalle de las normas internacionales para la práctica profesional de la auditoría interna.
ISACA	2009	Risk IT Framework	Orientación sobre cómo gestionar los riesgos relacionados con TI
ISACA	2014	CISA Review Manual	Contiene información detallada para la realización de auditoría de sistemas.
ISACA	2014	COBIT 5 Principales	Explicación detallada de los principios de Cobit 5

Autor	Año	Título	Aportes
ISACA	2014	ITAF, A professional Practice Framework for IS Audit/Assurance	Proporciona orientación, herramientas y técnicas sobre la planificación, el diseño, la realización de informes sobre la auditoría del sistema de información y las asignaciones de aseguramiento.
ISACA	2016	Information Systems Auditing: Tools and Techniques - Creating Audit Programs	Proporciona una guía con los pasos necesarios para lograr un entendimiento básico para la correcta realización de Programas de Auditoría.
Hans Henrik Berthing	2015	Using COBIT 5 for Assurance as Framework for your IT audit	Aplica los principios de COBIT 5 para Aseguramiento para la etapa de Planeación y Reporte de una Auditoría de Sistemas
ISACA	2016	Sample Audit and Assurance Program in 5 steps	Ejemplifica la elaboración de un plan de auditoría para una red privada virtual VPN
Manuel Ballester/ISACA	2010	Gobierno de las TIC ISO/IEC 38500	Brinda un breve resumen de la ISO IEC 38500
Norma sobre Gestión de Riesgo Tecnológico	2007	Superintendencia de Bancos y de Otras Instituciones Financieras.(Nicaragua)	El artículo no. 4 indica los criterios de información para el control y gestión de las tecnologías de la información. En su artículo no. 29 explica los controles de infraestructura que deben de aplicarse para el resguardar la seguridad física de componentes de TI, entre otros aportes.

Cuadro 1. Revisión bibliográfica.

CAPÍTULO I - ANÁLISIS DE LAS PRÁCTICAS ACTUALES DE LOS AUDITORES DE SISTEMAS EN LAS INSTITUCIONES BANCARIAS DE PRIMER PISO EN NICARAGUA.

Para analizar las prácticas actuales que implementan los auditores de sistemas de las instituciones bancarias de primer piso de Nicaragua realizamos una encuesta dirigida a estos auditores.

El propósito de la encuesta que realizamos para nuestra investigación lo describimos en los siguientes puntos:

1) Conocer si los equipos de auditoría cuentan con metodologías de trabajo formalmente definidas y documentadas.

2) Identificar si existe alguna tendencia en la implementación de alguna metodología en particular, en la ejecución de una auditoría de sistemas.

3) Determinar si en la práctica la realización de una auditoría se realiza de acuerdo a la(s) metodología(s) que previamente se hayan definido en la unidad de auditoría interna (si existe una metodología).

La encuesta realizada consta de 21 preguntas. Por lo cual se realizó el análisis de los resultados de las preguntas más importantes que hemos definido para el objetivo de nuestra investigación. Véase detalle de la encuesta en la sección de Anexos – **Anexo I – Encuesta sobre Auditoria de Sistemas**

1.1 Fases de la Auditoría

Un 66.7% de los encuestados estaban de acuerdo de que el proceso de auditoría podría segmentarse en cuatro fases: Planeación, Ejecución, Presentación de

Resultados y Seguimiento a las Oportunidades de Mejora. El 33.3% indicó que pueden haber otras fases.

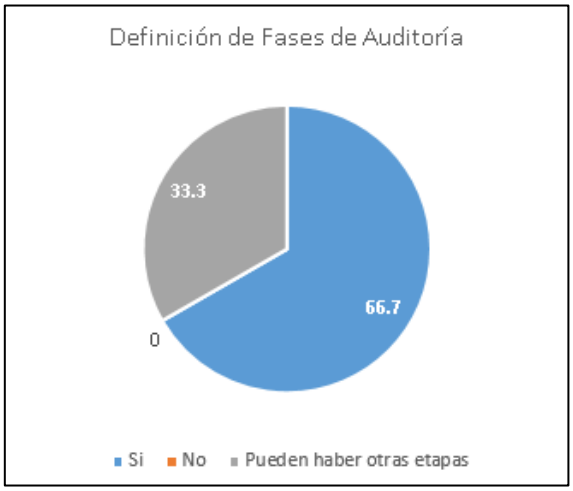


Gráfico 1. Definición de fases de auditoría

Este 33.3% indicó que otra etapa a considerarse es la Pre – Auditoría. Sin embargo, la etapa de pre – auditoría puede ser incluida como parte de la fase de Planeación. La metodología propuesta está basada en las cuatro fases indicadas anteriormente, apoyándonos en el estándar indicado por el marco de trabajo de ITAF.

El resto de preguntas de la encuesta están enfocadas en conocer cómo los auditores internos implementan o no las fases previamente definidas.

1.2. Planeación de la Auditoría

El 100% de los encuestados respondieron que sí cuentan con una metodología y/o instrumentos definidos para la realización de la Planeación de la auditoría. Los encuestados indicaron que el origen de la metodología utilizada por ellos para la planeación de la auditoría son los siguientes:

- Está definida en los manuales operativos de Auditoría Interna (83.3%)

- Fue creada basándose en la experiencia del equipo de auditoría interna (33.3%)
- Fue creada basándose en un marco de trabajo en específico (33.3%)

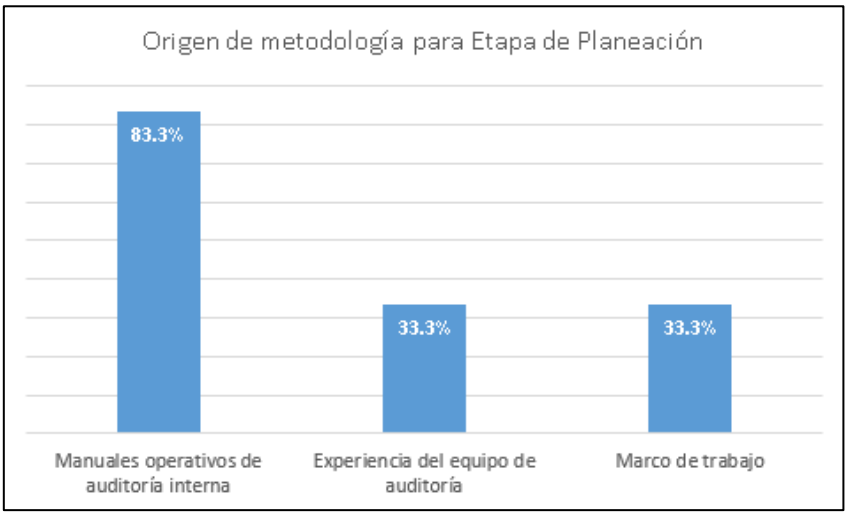


Gráfico 2. Origen de metodología para Etapa de Planeación.

Con lo anterior podemos inferir que en general los auditores internos sí poseen una metodología con la cual realizan la planeación de la auditoría y que la mayoría de ellos están asociados a manuales operativos internos previamente definidos.

Los auditores encuestados indicaron que en la etapa de Planeación de la auditoría realizan las siguientes actividades:

- Entendimiento del área y/o proceso a auditar.
- Reunión inicial con el área o unidad de negocio a auditarse.
- Definición de los objetivos generales y específicos de la auditoría.
- Definición del alcance de la auditoría.
- Revisión de manuales internos y normas de la SIBOIF.
- Revisión de auditorías previas.
- Elaboración de Matriz de Riesgo.
- Definición de actividades a realizar.

- Definición de las pruebas requeridas.
- Preparación del documento de planeación.

1.3. Ejecución de la Auditoría

El 100% de los encuestados indicaron que la fase de ejecución de la auditoría está basada en una metodología previamente definida en su departamento de auditoría interna. El origen de dicha metodología indicado por los encuestados es el siguiente:

- Políticas y Procedimientos de Control Interno.
- Marco de trabajo interno, en donde se definen las etapas de la auditoría interna y los formatos a utilizar.

Los auditores encuestados indicaron de manera general que las actividades realizadas en la fase de Ejecución son las siguientes:

- Informar y coordinar con el área a auditar los requerimientos de la auditoría.
- Realizar las actividades de acuerdo a lo inicialmente planificado.
- Ejecutar las pruebas previamente definidas y tomar las evidencias y soportes necesarios.
- Solicitar información complementaria en caso de ser necesaria y realizar análisis de la información.
- Recopilar información por varias vías.
- Realización de ayuda de memoria por las reuniones sostenidas con el personal del área a auditar.

Nota aclaratoria: Durante la etapa de Ejecución, pueden surgir cambios a los objetivos de la auditoría y por consiguiente cambios al plan inicial. Esto no fue indicado en ninguna de las respuestas sobre este punto, pero es importante para el conocimiento del lector que dichos cambios pueden surgir y son aceptables.

Los auditores indicaron que, para la fase de Ejecución, el marco de trabajo o metodología utilizado son generalmente Políticas y Procedimientos de Control Interno.

1.4. Presentación de Resultados

El 100% de los encuestados indicaron que la fase de Presentación de Resultados está basada en una metodología previamente definida en su departamento de auditoría.

El origen de la metodología empleada para la Presentación de Resultados indicada por los encuestados es la siguiente:

- Políticas internas.
- Manuales de auditoría interna.

Los auditores encuestados indicaron que la forma en que realizan esta fase es de la siguiente manera:

- Reunión y presentación de informe borrador (resultados preliminares).
- Presentación de hallazgos y observaciones.
- Elaboración de recomendaciones para obtener el plan de acción de cada punto encontrado.
- Presentación de las pruebas de conformidad.
- Presentación de los alcances planificados, desglose de los resultados conforme cada alcance, conclusión y recomendaciones.
- Presentación a nivel de resumen ejecutivo de las situaciones relevantes al Comité de auditoría.

Los instrumentos utilizados por los auditores encuestados para la Presentación de Resultados son los siguientes:

- Informe final.
- Documento con los Objetivos Generales, Objetivos Específicos, Pruebas y hallazgos encontrados.
- Presentación en Power Point.

1.5. Seguimiento a las Oportunidades de Mejora

Al consultar a los auditores internos si ejecutan o no la fase de Seguimiento a las Oportunidades de Mejora, respondieron lo siguiente:

- Si (50%)
- No (50%)

Gráfico 3. Implementación de etapa de seguimiento a oportunidades de mejora.

Los auditores que contestaron que sí ejecutan la fase de seguimiento a oportunidades de mejora indicaron que ejecutan esta fase de la siguiente manera:

- Revisar si existen observaciones anteriores que no hayan sido superadas por el área responsable.
- Realizar actividades de seguimiento durante el trabajo de campo.
- Presentar el estado de las oportunidades de seguimiento anteriores a la auditoria en el informe final.

1.6. Conclusión del análisis de la encuesta.

Analizando los resultados de la encuesta se logra evidenciar que cada equipo de auditoría interna ciertamente sí cuenta con una metodología previamente definida para la realización de auditorías, pero no conocen exactamente con cual marco de trabajo o prácticas están fundamentados, dado que la mayoría de sus herramientas y métodos están soportados por manuales internos previamente aprobados y en la realización de la labor de auditoría se apoyan justamente en los manuales internos.

Por la conclusión anterior vemos justificado nuestro trabajo investigativo, dado que, a como lo indicaron los encuestados, las prácticas de auditoría están sustentadas en documentación interna de la institución bancaria y por lo tanto no son de acceso público. Con esta investigación facilitaremos una propuesta metodológica que sea accesible al público interesado en conocer el cómo realizar el proceso de auditoría de sistemas y conocer cuáles son las bases metodológicas internacionales en las cuales se apoya dicha forma de trabajo.

CAPÍTULO II: PLANTEAMIENTO DE LAS ETAPAS DE LA AUDITORÍA DE SISTEMAS DE LA PROPUESTA METODOLÓGICA.

2.1. Introducción.

La realización de una auditoría de sistemas puede surgir por al menos una de las siguientes tres razones:

– Como parte de la ejecución del plan anual de auditoría.
– A solicitud de la Junta Directiva o Alta Gerencia de la Institución.
– A solicitud del Ente Regulador de la Institución.

El plan anual de auditoría contiene la naturaleza, el momento y el alcance de los procedimientos de auditoría que deben llevar a cabo los miembros del equipo de trabajo para obtener suficiente evidencia de auditoría apropiada para formar una opinión. El plan anual de auditoría incluye las áreas a ser auditadas, el tipo de trabajo planeado, los objetivos de alto nivel y el alcance del trabajo y temas como presupuesto, asignación de recursos, fechas programadas, tipo de informe, público objetivo y otros aspectos generales del trabajo.[35]

La Junta Directiva y/o la Alta Gerencia poseen la autoridad de solicitar la realización de auditorías internas para proceder con la revisión de un área y/o proceso específico. Por ejemplo, si a criterio de las partes interesadas (entiéndase Junta Directiva, Alta Gerencia) se requiere la revisión del sistema informático encargado del pago de intereses a los cuentahabientes del banco, ésta (la Junta Directiva) procede a solicitar de manera formal la realización de la revisión correspondiente al

[35] IS Audit and Assurance Guideline 2202 Risk Assessment in Planning . (n.d.). Recuperado el 07 de Octubre 2017 de http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/Guideline-2202-Risk-Assessment-in-Audit-Planning.aspx

departamento de Auditoría Interna. El personal de este departamento procedería con la planeación y ejecución de la auditoría solicitada.

La ley 316, Ley de la Superintendencia de Bancos y Otras Instituciones Financieras (SIBOIF), en su capítulo II indica que una de sus atribuciones es inspeccionar regularmente las instituciones que le corresponde, vigilar y realizar arqueos y otras verificaciones convenientes por medio del personal de la Superintendencia o el debidamente contratado para tal efecto. Estas inspecciones, arqueos y verificaciones deberán realizarse por lo menos una vez al año y podrán llevarse a cabo sin previo aviso a las instituciones a inspeccionar.[36]

Por lo anteriormente mencionado, la SIBOIF puede solicitar que se realice la revisión correspondiente de un proceso determinado y el equipo de auditoría interna debe de realizar las debidas diligencias para ejecutar dicha revisión. Una vez concluida la auditoría interna, SIBOIF puede proceder con la revisión de los informes generados por dicha auditoría.

2.1.1. Aspectos legales y normativos.

La Superintendencia de Bancos y Otras Instituciones Financieras, en su resolución no. CD-SIBOIF-500-1-SEP19-2007 define la Norma sobre Gestión de Riesgo Tecnológico. Esta norma está disponible para ser descargada desde el sitio web de SIBOIF (http://www.siboif.gob.ni). Su objetivo es establecer los criterios mínimos de evaluación sobre la administración de los riesgos, la seguridad, la utilización y los controles aplicativos de la tecnología de la información de las entidades supervisadas.[37]

[36] Ley No. 316. La Gaceta, Diario Oficial de la República de Nicaragua, No.196 ,14 octubre 1999
37 Norma sobre Gestión de Riesgo Tecnológico (SIBOIF), Artículo 2, 19 de septiembre 2007.

Es importante que el auditor de sistemas de una institución financiera conozca cuáles son los criterios definidos por esta norma de SIBOIF. En su artículo no. 4, esta norma establece que los criterios de información para el control y gestión de las tecnologías de la información y sus riesgos asociados son: confiabilidad, confidencialidad, disponibilidad, efectividad, eficiencia e integridad. En este aspecto, el auditor de sistemas debe implementar una metodología que le permita lograr evidenciar que los criterios anteriormente mencionados son cumplidos por el proceso que está evaluando.

En su artículo 27, esta norma se refiere a la seguridad lógica que debe de ser definida por las instituciones financieras. Los controles que deben de implementarse, asociados a la seguridad lógica, incluyen políticas de limitación y control de acceso a programas, bases de datos, servicios de redes y sistemas operativos. Estos tipos de controles aplicativos son objeto de evaluación en la realización de auditoría de sistemas y por lo tanto, el auditor debe considerar en sus pruebas de campo la verificación del cumplimiento de este requerimiento establecido por SIBOIF.

Otro artículo importante a considerar es el no. 29, el cual se refiere a la seguridad física y ambiental. En lo que respecta a la seguridad física podemos considerar los controles diseñados para evitar el acceso a instalaciones o áreas restringidas (control de acceso) con el fin de mitigar daños e intrusiones. Además del control de acceso a instalaciones físicas, este artículo define otros objetivos relacionados a reducir el riesgo de acceso no autorizado a medios de almacenamiento e instalaciones de procesamiento de información.

En resumen, el auditor de sistemas de una institución financiera regulada por SIBOIF, debe leer y analizar el contenido de la Norma sobre Gestión de Riesgo Tecnológico debido a que es el soporte legal sobre el cual se implementan y validan

los controles necesarios para mitigar los riesgos inherentes a las tecnologías de la información de la institución financiera.

Los artículos de esta norma pueden ser considerados como una serie de lineamientos que deben de ser implementados y cumplidos en un nivel aceptable por parte de la Gerencia de TI, pero no presenta de una forma concreta bajo qué mecanismos debe de llevarse a cabo la evaluación de los criterios expuestos en sus distintos artículos. En la propuesta realizada en nuestra investigación, recomendamos la lectura de esta Norma de Riesgo Tecnológico, la cual aportará al auditor una base teórica sobre los aspectos legales que deben de ser tomados en cuenta al momento de realizar una auditoría de sistemas en una institución bancaria.

2.1.2. Objetivos estratégicos de la organización.

El primer principio de Cobit 5, el cual es “Satisfacer las necesidades de las partes interesadas”, expresa la necesidad de alinear los objetivos y prioridades individuales y departamentales con los de la organización y así lograr los objetivos estratégicos de la entidad.[38]

En el cumplimiento de los objetivos estratégicos de la organización participan tanto las personas individuales así como los departamentos o gerencias a los cuales pertenecen. La estrategia de la Gerencia de TI debe estar alineada con los objetivos estratégicos de la organización, pero ciertamente, esta gerencia está enfocada en ofrecer servicios que soporten la operatividad de las demás áreas de la entidad. Por lo tanto, surge la necesidad de que todas las áreas de la organización estén alineadas con la estrategia de las partes interesadas debido a que esto permite el uso óptimo de los recursos del departamento de tecnología de la información.

[38] ISACA (2014).Cobit 5 principles: Where did they come from? [White paper]. P.5

Debido a que la mayoría de los procesos de las distintas áreas de negocios están automatizados, la auditoría de sistemas permite validar que dichos procesos cumplan con su funcionalidad en un nivel razonable. Los procesos de negocio deben estar enfocados en la generación de valor a la institución, en la reducción de costos y en la optimización de los recursos y, por lo tanto, el poder validar estos procesos permite garantizar que las distintas áreas de negocio cumplan con sus funciones de la mejor manera posible.

La metodología presentada en nuestra investigación parte del supuesto de la previa existencia de un plan estratégico definido, de un plan de auditoría anual en la institución y que ya se han definido con anterioridad los objetivos de auditoría. Excluimos de nuestra metodología el proceso de la elaboración del plan anual, así como la implementación del cumplimiento de los objetivos estratégicos porque está fuera del alcance de nuestra investigación (nuestra investigación está orientada principalmente a la realización de la auditoría de sistemas).

2.2. Etapas del proceso de auditoría de sistemas.

Partiendo de los estándares de auditoría y aseguramiento propuestos por el marco de trabajo ITAF[39] (ISACA), basaremos nuestra metodología en cuatro fases del proceso de auditoría: Planeación, Ejecución, Presentación de Resultados y Seguimiento.

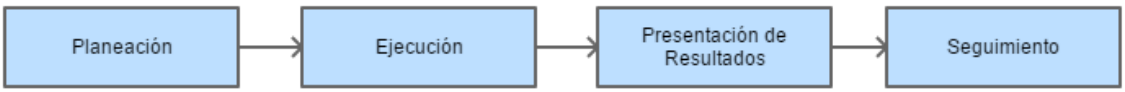


Diagrama 1: Fases de Auditoría

[39] Information Technology Assurance Framework (ITAF)

2.2.1. Planeación

En la fase de planeación[40] el auditor interno debe de preguntarse ¿qué pretendemos lograr con la auditoría?, ¿cuáles son los objetivos de la auditoría que realizaremos? ¿Qué actividades tendremos que realizar para cumplir con los objetivos de la auditoría? ¿Con qué recursos contamos para poder llevar a cabo la auditoría y completarla en el tiempo esperado? Es en esta etapa que se elabora el programa de auditoría.

2.2.2. Ejecución

La etapa de ejecución[41] se trata de la realización de todas las actividades definidas en el programa de auditoría , es decir, entrar en el campo a auditar, realizar las tomas de datos requeridas y obtener todas las evidencias necesarias que soporten dicho trabajo de auditoría. En esta etapa también se debe de preparar toda la documentación necesaria para su posterior presentación.

2.2.3. Presentación de Resultados

En la etapa de presentación de resultados[42] el auditor debe de generar los informes con todos los comentarios y recomendaciones.

2.2.4. Seguimiento a Oportunidades de Mejora

Finalmente, en la etapa de seguimiento[43] el auditor debe monitorear y asegurar que se han tomado las medidas necesarias para superar las oportunidades de mejoras y /o hallazgos reportados.[44]

---

[40] ISACA (2014) . ITAF: A Professional Practices Framework for IS Audit/Assurance, IS Audit and Assurance Standard 1201 Engagement Planning

[41] ISACA (2014) . ITAF: A Professional Practices Framework for IS Audit/Assurance,IS Audit and Assurance Standard 1203 Performance and Supervision

[42] ISACA (2014) . ITAF: A Professional Practices Framework for IS Audit/Assurance,IS Audit and Assurance Standard 1401 Reporting,Key Aspects

[43] ISACA (2014) . ITAF: A Professional Practices Framework for IS Audit/Assurance,IS Audit and Assurance Standard 1402 Follow-up Activities, Keys Aspects

[44] ISACA (2014) . ITAF: A Professional Practices Framework for IS Audit/Assurance,IS Audit and Assurance Standard 1402 Follow-up Activities, Statement 1402.1

2.3. Marco de trabajo a implementar.

Nuestra metodología la basaremos en el marco de trabajo ITAF (A Professional Practices Framework for IS Audit/Assurance), 3ra Edición y aspectos aplicables de GTAG (Global Technology Audit Guide - Guías de Auditoría de Tecnología Global) de la organización IIA (The Institute of Internal Auditors); siendo importante mencionar también en la tropicalización de las mejores prácticas de auditoría y cúmulos de experiencias.

ITAF[45] es un modelo de referencia integral y de buenas prácticas que:

- Establece estándares que abordan los roles y responsabilidades profesionales de auditoría y aseguramiento de SI; conocimientos y habilidades, diligencia, conducta y requisitos de informes.
- Define los términos y conceptos específicos de aseguramiento de SI.
- Proporciona orientación y herramientas y técnicas sobre la planificación, el diseño, la realización y el informe de las asignaciones de auditoría y aseguramiento de SI.

Las GTAG (Guías de Auditoría de Tecnología Global), las cuales son consideradas por el Instituto de Auditores Internos (IIA) - GTAG 1[46] la cual consiste en explicar los riesgos y controles de TI en un formato que permite a los jefes ejecutivos de auditoría y a los auditores internos comprender y comunicar la necesidad de poseer fuertes controles de TI. Los controles de TI son esenciales para proteger activos, clientes, socios e información sensible; demostrar seguridad, eficiencia y comportamiento ético, reputación y confianza.

[45] ISACA (2014) . ITAF: A Professional Practices Framework for IS Audit/Assurance. Introduction
[46] IIA (2012). Global Technology Audit Guide (GTAG®) 1 Information Technology Risk and Controls 2nd Edition. p. 3

2.4. Lineamientos implementados

Para definir las etapas de la auditoría en nuestra metodología nos apoyamos en el contenido de los estándares propuestos por ITAF. En el siguiente cuadro observamos los estándares implementados en cada una de las etapas:

Estandar ITAF	Declaraciones (descripción breve)
Presentación de resultados **1401. Reporting (Reportes)**	**1401.1** - Los profesionales de auditoría y aseguramiento de SI deberán proporcionar un informe para comunicar los resultados al finalizar el trabajo
	1401.2 - Los profesionales de auditoría y aseguramiento de SI deberán garantizar que los hallazgos en el informe de auditoría cuenten con el respaldo suficiente y con las apropiadas pruebas de auditoría.
Seguiento a oportunidades de mejora **1402.** Follow up Activities (Actividades de seguimiento)	**1402.1** - Los profesionales de auditoría y aseguramiento de SI deberán monitorear la información relevante para concluir si la gerencia ha planificado / tomado acción apropiada y oportuna para abordar los hallazgos y recomendaciones de auditoría informados.

Estandar ITAF	Declaraciones (descripción breve)
Planeación **1201**. Engagement Planning (Planificación del trabajo)	**1201.1** - Los profesionales de Auditoría de Sistemas Informáticos deberán planear cada etapa del proceso de auditoria.
	1201.2 - Los profesionales de Auditoría de Sistemas Informáticos deben desarrollar y documentar un plan de proyecto de auditoría.
Ejecución **1203.** Performance and Supervision (Ejecución y supervisión)	**1203.1** - Se realizará el trabajo de acuerdo con el plan de auditoría aprobado para cubrir los riesgo y dentro del cronograma acordado.
	1203.2 - Los auditores de SI deberán proporcionar supervisión al personal de auditoría para los casos aplicables.
	1203.3 - Los auditores de SI aceptarán solo tareas que estén dentro de sus conocimientos y habilidades.
	1203.4 - Los auditores de SI obtendrán evidencia suficiente y apropiada para lograr los objetivos de la auditoría.
	1203.5 - Los auditores de SI deben documentar el proceso de auditoría, describiendo el trabajo y la evidencia de auditoría que apoya hallazgos y conclusiones.
	1203.6 - Los auditores de SI deberán identificar los hallazgos y obtener conclusiones a partir de los mismos.

Cuadro 2. Etapas propuestas en el proceso de auditoría de sistemas (continuación).

CAPÍTULO III. FUNDAMENTOS DEL DESARROLLO DE LA METODOLOGÍA E INSTRUMENTOS PROPUESTOS.

A continuación indicaremos la base teórica con la cual soportamos el desarrollo de cada una de las etapas de la auditoría de sistemas propuesta en nuestra metodología y de la misma forma indicaremos una serie de instrumentos que ayudarán al auditor a llevar un control de las actividades de cada etapa de la auditoría.

3.1. Etapa de Planeación

Cada institución posee un conjunto de unidades de negocio que realizan una serie de operaciones, las cuales pueden o no estar coordinadas entre sí, con el fin de poder cumplir con los objetivos que hayan definido la Junta Directiva y/o la Alta Gerencia y así llevar a cabo sus planes de negocio de manera satisfactoria.

Estas unidades de negocio poseen un conjunto de procesos pero los más relevantes de la institución deben de formar parte del Universo de Auditoría, el cual no es más que el conjunto de procesos que se pueden tener en cuenta para la ejecución de auditorías. Podría decirse también que el Universo de Auditoría sirve como la fuente a partir de la cual se prepara el plan de auditoría anual.[47]

ISACA recomienda una serie de pasos para la elaborar el Plan de Auditoría:[48]

- Determinar el tema de auditoría.
- Definir el objetivo de auditoría.

[47] ISACA Glossary Terms: Audit Universe. (n.d.). Retrieved October 07, 2017, from http://www.isaca.org/Knowledge-Center/Lists/ISACA%20Glossary%20Terms/DispForm.aspx?ID=1011

[48] Excerpted from ISACA White Paper, Information Systems Auditing: Tools and Techniques—Creating Audit Programs (www.isaca.org/creating-audit-programs)

- Establecer el alcance de la auditoría.
- Realizar planificación previa.
- Determinar los pasos para la recolección de datos.

Es muy importante en la etapa de planeación hacer un análisis de riesgo de los procesos a auditar.

3.1.1. El análisis de riesgo en la etapa de planeación

En nuestra metodología proponemos que en la etapa de planeación se ejecute el Análisis de Riesgo, el cual nos debe permitir identificar y evaluar de manera apropiada los riesgos en los procesos que serán auditados.

La GTAG 1 indica que para la ejecución del análisis de riesgo el auditor puede plantearse una serie de preguntas:[49]

- ¿Qué activos de TI (esto incluye tanto tangibles como activos de TI intangibles, así como información o reputación) están en riesgo, y cuál es el valor de su confidencialidad, integridad y disponibilidad?
- ¿Qué evento puede afectar los activos de información? Qué vulnerabilidades hay que puedan afectar de manera negativa la información de la institución (robo de información, ingreso no autorizado a información sensible, etc.)?
- Si ocurriera un evento de amenaza, ¿qué tan malo puede ser el impacto de dicho evento?
- ¿Con qué frecuencia se espera que ocurra dicho evento (frecuencia de ocurrencia)?

[49] IIA (2012). Global Technology Audit Guide (GTAG®) 1 Information Technology Risk and Controls 2nd Edition. p. 11

- Cuán ciertas son las respuestas a las primeras cuatro preguntas? (análisis de incertidumbre)
- ¿Qué puede hacerse para reducir el riesgo?
- ¿Cuánto costará reducir el riesgo?
- ¿Es rentable el reducir el riesgo?

De la misma manera, GTAG 1 propone las siguientes estrategias para mitigar los riesgos:

- Aceptar el riesgo: cuando el riesgo es muy bajo o el mitigar el riesgo implica un costo demasiado alto, se puede aceptar su existencia, siempre y cuando se esté monitoreando periódicamente para validar que dicho riesgo continúa siendo bajo y/o su costo de mitigación no es rentable para el negocio.

- Eliminar el riesgo: es posible que un riesgo esté asociado con el uso de una tecnología o proveedor. El riesgo puede ser eliminado cambiando dicha tecnología o proveedor y reemplazándolos por opciones más robustas.

- Compartir el riesgo: Los enfoques de mitigación de riesgos pueden ser compartido con socios comerciales y proveedores. Esto quiere decir que, por ejemplo, si en la empresa hay un centro de datos con equipo de alta tecnología (y costosa) es mejor contratar a otra empresa que posee personal mejor calificado que se encargue de administrar dicho centro de datos. En ese caso, el riesgo es compartido con la empresa que ofrece el servicio de outsourcing.

- Controlar/Mitigar el riesgo: En lugar de - o en combinación con - otras opciones, los controles pueden idearse e implementarse para prevenir el riesgo de manifestarse para limitar la probabilidad de dicho riesgo ocurra o minimice sus efectos.

3.1.2. **Desarrollo de la Planeación de Auditoría de sistemas bajo nuestra propuesta metodológica.**

Para la etapa de Planeación proponemos realizar los siguientes instrumentos, mismos que se utilizan para el entendimiento del proceso a auditar:

A. Entendimiento del Proceso a Auditar

A como se ha indicado en la sección anterior, una de las primeras herramientas a utilizar dentro de la Fase de la Planeación está relacionada con el entendimiento del proceso a Auditar; por lo cual se propone la plantilla **"Formato de Requerimientos Iniciales" – Ver Anexo II**; el cual va dirigido al Gerente del Área a Auditar.

A través de esta herramienta, se da inicio a un vínculo o interacción formal con el Auditado, sin embargo (en dependencia de la necesidad), también se puede iniciar con otra herramienta la que puede ser una **"Entrevista de Reunión Inicial"** misma que debe quedar sustentada en los papeles de trabajo del Auditor, ver "**Formato de Ayuda Memoria**" en **Anexo III.**

Dentro de la fase de la planeación de Auditoría es importante mencionar que existe una relación directa entre los procesos que se requieren auditar y el alcance de la Auditoria que se define en los objetivos de Auditoria, siendo importante destacar que una de las herramientas fundamentales es el "Recorrido de Proceso" o "Walkthrough".

Los elementos que pueden servir para elaborar el recorrido del proceso pueden soportarse con los Manuales de Políticas y Procesos propios del área, entrevistas con el personal que interviene en el proceso, pruebas de observación, entre otros.

Por ende la evaluación de los procesos puede ser evaluada a manera de resumen en:

1) Entendimiento del Proceso,

2) Identificación de los Riesgos y Controles del Proceso,

3) Selección de los controles relevantes a los que se realizaran las pruebas (Alcance de Auditoría) – Se expresa en la sección

4) Evaluación del diseño y la implementación de los controles (Constatar si los controles existentes son efectivos y eficientes)[50]

Las evidencias del recorrido del proceso o Walkthrough pueden quedar documentadas a través de un análisis de brechas o GAP en el cual pueden determinarse las variaciones existentes entre lo que se tiene documentado en los procedimientos internos y las actividades realizadas en la práctica por el personal que los ejecuta, puede verse en el **Anexo IV – Análisis de Brecha o GAP.**

La Matriz de Riesgo es un complemento importante dentro de la planeación de Auditoria que permite englobar en una sola herramienta el entendimiento que se ha obtenido, mismo que nos permite visualizar la alineación que abarca el negocio, conexo con los procesos, riesgos y controles en cada línea de trabajo, a continuación se propone a manera de ejemplo una matriz de riego conteniendo los componentes principales que deben considerarse, véase **Anexo V – Matriz de Riesgos.**

[50] **Ver referencia:** www.auditool.org/blog/auditoria-externa/219-como-generar-valor-agregado-a-nuestros-clientes-mediante-la-evaluacion-de-los-procesos.

B. Definición de los Objetivos y el Alcance de la Auditoría

Una vez conocido el entorno del proceso a auditar y por ende el giro del negocio, proponemos la herramienta "**Planeación de Trabajo**" véase **Anexo VI**, dentro de esta parte es importante destacar que el alcance debe ser suficiente para lograr los objetivos de la revisión y para ello debe tomarse en cuenta los sistemas de información, en complemento con las personas involucradas en el proceso, activos, entre otros.

En la parte de la definición del alcance de la Auditoria se determina si es aplicable a realizar dentro de la Auditoria de TI, una revisión de Controles Generales o de Controles Específicos [*esta terminología está expresada en el Capítulo I, literal B, numeral 7.1 y 7.2*] o bien dentro de lo que es el término de Auditorias Integrales a manera de complemento en una auditoria en específico.

C. Elaboración del Programa de Auditoría

El programa de Auditoría, es el procedimiento a seguir, en el examen a realizarse, el mismo que es planeado y elaborado con el apoyo de las secciones indicadas anteriormente y el contenido debe ser flexible, sencillo y conciso, de tal manera que los procedimientos a ser empleados en la Auditoría estén de acuerdo con las circunstancias del examen.

Es importante destacar el hecho de no existir una norma o patrón exclusivo para elaborar el programa de Auditoría, lo cual no excluye la existencia de normas generales que se aplican a todos los casos y que constituyen los fundamentos de la técnica de la Auditoría en un determinado sector. Por lo tanto no se debe perder de vista que este debe ser una guía segura e indicadora de lo que deberá ser hecho y posibilite la ejecución fiel de los trabajos de buen nivel Profesional, que acompañe el desarrollo de tal ejecución.

Existen muchas formas y modalidades de un programa de Auditoría, desde el punto de vista del grado de detalle a que llegue, se les clasifica en programas generales y programas detallados. Los programas de Auditoría generales, son aquellos que se limitan a un enunciado genérico de las técnicas a aplicarse, con indicación de los objetivos a alcanzarse, y son generalmente destinados a uso de los jefes de los equipos de Auditoría. Los programas de Auditoría detallados, son aquellos en los cuales se describen con mayor minuciosidad la forma práctica de aplicar los procedimientos y técnicas de Auditoría, y se destinan generalmente al uso de los integrantes del equipo de Auditoría.

Resulta difícil establecer una línea divisoria entre los programas de Auditoría generales y detallados, la aplicación de uno u otro programa debe obedecer a las características del trabajo a efectuarse, a la forma de organización de la Sociedad de Auditoría que la va realizar, a los procedimientos de supervisión que tiene establecido la Sociedad Auditora, y las políticas generales de la propia Sociedad. [51]

Con la explicación de lo que conlleva el realizar el Programa de Auditoria, a manera de ejemplo proponemos los componentes principales que lo contienen, siendo en este punto en específico para el desarrollo de nuestra propuesta de contextualización, un programa que permita ayudar a comprender al lector su elaboración; ejemplificando para ello un programa de auditoría para realizar una auditoría de sistema al módulo de caja de una institución financiera de primer piso.

En esta parte de nuestra investigación se propone el programa, mismo que será retomado en la siguiente sección “Etapa de la Ejecución de la Auditoria”, Véase en “**Anexo VII** - **Programa de Auditoria**”

[51] Resumen tomado de www.auditool.org/programa_de_auditoria

En resumen, las actividades e instrumentos propuestos para realizar la etapa de Planeación son las siguientes:

Actividades propuestas	Instrumentos de soporte	Ubicación
Entendimiento del proceso a auditar	Formato de Requerimientos Iniciales	Anexo II
	Entrevista de Reunión Inicial	Anexo III
	Formato de ayuda de memoria	Anexo III
	Análisis de brecha o GAP	Anexo IV
	Matriz de Riesgo	Anexo V
Definición de los Objetivos y el Alcance de la auditoría	Planeación del trabajo	Anexo VI
Elaboración del Programa de Auditoría	Programa de auditoría	Anexo VII

Cuadro 3. Actividades e instrumentos propuestos para la etapa de Planeación.

3.2. Etapa de la Ejecución.

En la ejecución de la auditoría pueden utilizarse varios documentos que respaldan los exámenes, las comprobaciones, las solicitudes, verificaciones in situ, muestras, cálculos, entre otros, las cuales pueden ser evidencias confeccionadas por el auditor, o suministradas internamente por el auditado o por un tercero.

Nota aclaratoria: El trabajo desarrollado durante la fase de planificación, normalmente se documenta a través de los generalmente conocidos como "papeles de trabajo o Works Papers - Pts" y también se documenta cada fase de auditoría; la ejecución de la Auditoria se referencia en el Programa de Auditoría que se ejemplificó en el ítems anterior "Elaboración del Programa de Auditoria".

A. Principales herramientas para la ejecución de la Auditoría

Para efecto de nuestra propuesta, se proponen las siguientes herramientas basadas en las mejoras prácticas, a continuación el detalle de las principales herramientas:

1- **Los cuestionarios**:

Es una herramienta para iniciar el desarrollo de las Auditorias los cuales permiten obtener información y documentación de todo el proceso de una organización, igualmente aplican en la fase de Planeación desde el enfoque de entendimiento del proceso. El auditor debe realizar una tarea o actividad de campo para obtener la información necesaria, basado en las **evidencias** o hechos demostrables. Estas herramientas puede omitirse si el auditor ha podido recabar la información por otro medio.

2- **La entrevista:**

Con esta herramienta se obtiene información más específica, utilizando el método del **interrogatorio**, con preguntas variadas y sencillas, pero que han sido convenientemente elaboradas.

3- **Check-list (Listas de comprobación):**

Conjunto de preguntas y/o atributos las cuales se ejecutan con base en la observación o comparación entre los procedimientos documentados y los realizados en la práctica, véase un ejemplo de la herramienta en el **Anexo VIII**. Cabe destacar que esta herramienta puede utilizarse y adaptarse de diversas maneras de conformidad con el propósito requerido.

4- Selección de la Muestra a Revisar

La norma internacional de auditoría 530 trata del uso del muestreo de auditoría estadístico y no estadístico cuando el auditor ha decidido usar muestreo de auditoría.

Esto implica el diseño y selección de la muestra de auditoría, desarrollando pruebas de control y pruebas de detalle, evaluando los resultados de la

muestra, véase en Anexo IX el ejemplo de calcular el tamaño de la muestra. Cabe destacar que para determinar el tamaño de la muestra se pueden considerar un sin número de herramientas existentes entre las cuales tenemos software especializados como Idea Datos y/o páginas de internet especializadas en el tema.

Cuando el auditor decide usar muestreo de auditoría, su objetivo es proporcionar una base razonable para extraer conclusiones sobre la población de la que se selecciona la muestra.

Diseño de la muestra, tamaño y selección de partidas para prueba: El auditor debe establecer el propósito del procedimiento de auditoría cuando diseña una muestra de auditoría, teniendo en cuenta las características de la población, y el uso de enfoques estadísticos y no estadísticos.

Igualmente el auditor debe determinar el tamaño de la muestra, reduciendo el riesgo de muestreo a un nivel aceptable bajo; y seleccionar los items que le permitan representar la población entera; entre menor sea el riesgo que el auditor determine aceptar, mayor debe ser el tamaño de la muestra. El auditor puede determinar apropiado la estratificación de la población de acuerdo a las características de la misma.[52]

Existen varios métodos que el auditor puede utilizar para la selección de la muestra, como son:

- **Selección aleatoria:** Selección mediante generadores de números aleatorios.

- **Selección sistemática:** El número de unidades de muestreo en la población se divide entre el tamaño de la muestra para dar un intervalo de muestreo.

[52] Resumen obtenido de www.auditool.org – Muestreo de Auditoría

- **Muestreo por unidad monetaria:** Selección por valor ponderado, en la cual el tamaño de la muestra, selección y evaluación den como resultado una conclusión en montos monetarios.

- **Selección fortuita o casual:** El auditor selecciona una muestra sin seguir una técnica estructurada.

- **Selección en bloque:** Selección de uno o más bloques de partidas contiguas de la población.

5- Ejecución de la auditoría, de acuerdo a los objetivos inicialmente planteados.

En la etapa de ejecución, el auditor debe apegarse a los objetivos de auditoría definidos previamente en la etapa de planeación. Para lograr los objetivos, el auditor puede apoyarse en la revisión de los controles aplicativos correspondientes al área de negocio auditado, por lo tanto, entre las actividades a realizar puede incluirse la revisión de bitácoras, la verificación de la correcta separación de funciones en el departamento de TI, la revisión del control de versiones del código fuente de la aplicación evaluada, entre otros.

En resumen, para la etapa de Ejecución de la auditoría, proponemos las siguientes actividades:

Instrumento de soporte	Descripción	Ubicación
Cuestionarios	A criterio del auditor y en concordancia con los objetivos de auditoría	-
Entrevistas	A criterio del auditor y en concordancia con los objetivos de auditoría	-

Instrumento de soporte	Descripción	Ubicación
Checklist	Se realiza por revisión visual y/o comparación de atributos.	Anexo VIII
Selección de muestra	Según formato sugerido en nuestra propuesta	Anexo IX.

Cuadro 4. Instrumentos propuestos para la etapa de Ejecución.

3.3. Etapa de la Presentación de los Resultados

En el transcurso de una auditoría, los auditores designados a la revisión, mantendrán constante comunicación con los Auditados de la Institución Financiera, dándoles la oportunidad para presentar pruebas documentadas, así como información verbal pertinente respecto de los asuntos sometidos a examen; la comunicación de los resultados se la considera como una de las última fase de la auditoría, sin embargo debe ser ejecutada durante todo el proceso.

Al finalizar los trabajos de auditoría en el campo, se dejará constancia documentada de que fue cumplida la comunicación de resultados en los términos previstos de acuerdo a la fase de planeación de la auditoria o bien por la normas en caso de aplicar y su ley en materia".

En esta fase se procede a la elaboración del informe, en donde el equipo de auditoría comunica a los funcionarios de la entidad auditada los resultados obtenidos durante todo el proceso de ejecución de la auditoría, **Véase en Anexo X** - **Formato de Presentación de Resultados**, conteniendo los principales elementos de acuerdo a mejores prácticas. Es importante mencionar que existen ocasiones en las cuales el funcionario puede requerir de un resumen ejecutivo.

3.4. Etapa de Seguimiento a Oportunidades de Mejora

La Unidad de Auditoría Interna (UAI) deberá efectuar el seguimiento a las oportunidades de mejoras emitidas y comunicadas a la Gerencia encargada de implementarla (el seguimiento es continuo hasta que se implemente por completo).

Es importante destacar que para dar por cumplidas las oportunidades de mejora se deben de obtener y validar los soportes correspondientes que sean suficientes para atender integralmente la observación. El seguimiento se puede presentar ante el Comité de Auditoría y/o Junta Directiva con periodicidad mensual trimestral, etc. Véase en **Anexo XI** la propuesta de una matriz para efectuar el seguimiento a las oportunidades de mejoras.

El seguimiento a las oportunidades de mejora es recomendable que se acompañe con un informe de seguimiento para el cual puede utilizarse el formato indicado en el **Anexo X**. Véase a continuación una propuesta de cómo puede presentarse un resumen a una fecha corte determinada.

Órgano emisor	**Recomendaciones en proceso al DD/MM/YYYY**	**Movimientos al corte de la auditoria de seguimiento**		**Recomendaciones en proceso al DD/MM/YYYY**
		Nuevas	**Concluidas**	
SIBOIF	7	2	4	5
Auditoria Externa	66	41	21	86
Auditoría Interna	40	28	40	28
Otros	3	2	1	4
Total	**116**	**73**	**66**	**119**

Nota: Las cifras expuestas son de referencia para uso didáctico

CAPÍTULO IV. CONTEXTUALIZACIÓN DE LA PROPUESTA METODOLÓGICA PARA EJECUTAR LA AUDITORIA DE SISTEMA A UN MÓDULO DE CAJA.

4.1. Contextualización de la etapa de Planeación.

La realización de una auditoría de sistemas dentro de una institución financiera se desprende del Plan Anual de Auditoría o a como se indicó en secciones anteriores, como parte de un requerimiento del Comité de Auditoria, entre otros. En este plan se definen las distintas áreas y/o procesos que serán evaluados por el departamento de auditoría interna.

Para iniciar formalmente la etapa de Planeación de la auditoría, se propone la implementación del formato **"Requerimientos Iniciales de Auditoría"**:

Unidad de Auditoría Interna (UAI)
Centro Corporativo BancoABC
Teléf. XXXXXXXX
Managua, Nicaragua
http://www.bancoABC.com.ni

Banco ABC

<<Describir la fecha de inicio de la auditoria>> Managua, XX de Mes de 20XX

Sr. *<<Describir el Nombre del Gerente >>*
<<Describir la Gerencia>>
Su despacho

Estimado Sr. *<<Describir el Nombre del Gerente>>*:

De conformidad con las actividades programadas en nuestro plan anual de trabajo para el año 20XX, le informaos que hemos iniciando la revisión de *<<Describir la Actividad/Auditoría>>* con fecha de corte al XX de Mes de 20XX.

Para esta revisión ocasión acreditamos al siguiente Staff:

1. <<Describir el Nombre del Supervisor>>
2. <<Describir el Nombre del Auditor Encargado >>
3. <<Describir el Nombre del Auditor Encargado de Sistemas>>
4. [...]

Para desarrollar esta actividad requerimos de su Visto Bueno para iniciar el recorrido del proceso en las actividades que se realiza en el *<<Describir la Gerencia/Área>>* a revisar.

De ser necesario requerir información adicional, la estaremos solicitando con anticipación durante nuestra auditoria.

Con este formato se pretenden los siguientes tres aspectos principales:

- Expresar al gerente/responsable de área que se realizará un recorrido del proceso a auditar para identificar posibles brechas y/o identificación de riesgos no conocidos.
- Presentar el equipo que realizará la auditoría.
- Expresar al auditado la posibilidad de requerir mayor información que se necesita como insumo, para realizar la auditoría; se solicita de manera formal.

Una vez que se analiza los insumos iniciales, es recomendable solicitar una reunión inicial, la cual ayudará al auditor a comprender el alcance del proceso a revisar, dejando abierta la posibilidad de otras entrevistas y/o reuniones. Para poder soportar la realización de estas reuniones se propone el formato “Ayuda de memoria”:

Unidad de Auditoría Interna (UAI)
Centro Corporativo BancoABC
Teléf. XXXXXXXX
Managua, Nicaragua
http://www.bancoABC.com.ni

Banco ABC

<<Describir la fecha de inicio de la auditoria>> Managua, XX de Mes de 20XX

AYUDA MEMORIA

<<Describir los asistentes de la reunión>>

Núm.	Nombre	Firma
1	*<<Describir el Nombre del Gerente >>, <<Describir el Cargo del Gerente >>*	
2	*<<Describir el Nombre del Vice Gerente >>, <<Describir el Cargo del Vice Gerente >>*	
4	*<<Describir el Nombre del Auditor Supervisor >>*	
5	*<<Describir el Nombre del Auditor Encargado>>*	

TEMA: *<<Describir el Tema Principal de la Reunión Inicial>>*

A- **Resumen** *<<Describir el Resumen de los temas abordados en la reunión >>*

Nota Aclaratoria: El resumen puede ser elaborado de la manera más sencilla, la cual les permita recalcar las partes más importantes de la Reunión, en ella se pueden indicar requerimientos adicionales del Gerente, se pueden considerar temas de riesgo y control, y brechas inidentificadas durante un proceso de análisis GAP.

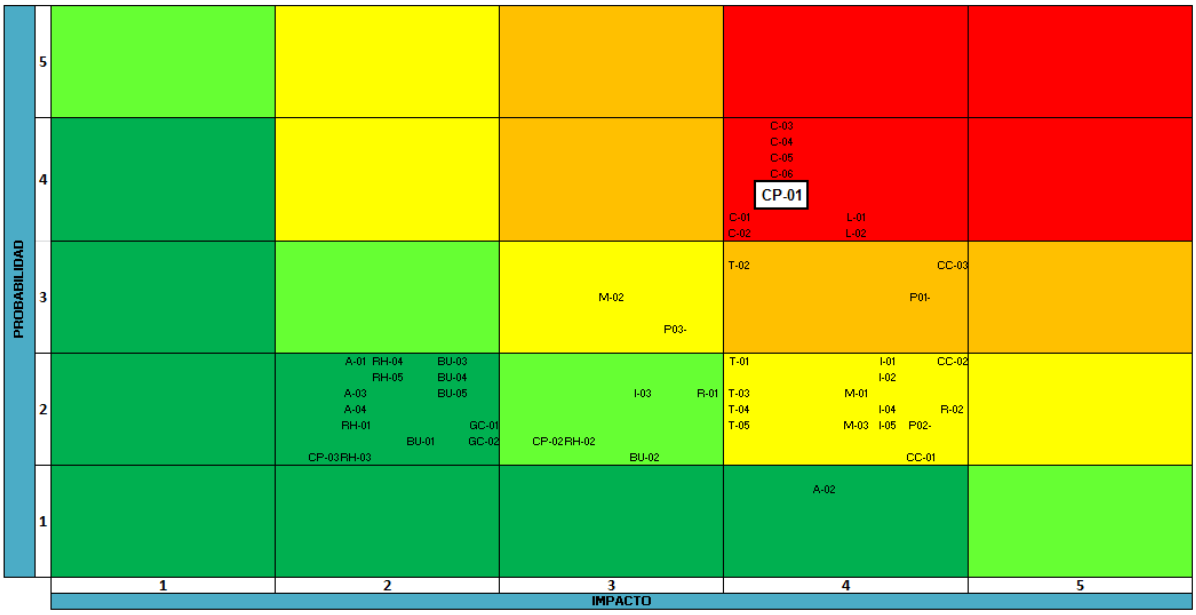
B- **Conclusiones / Acuerdos** *<<Describir la conclusión y o acuerdos asumidos como parte de la Reunión >>*

Con dicho formato “Ayuda de memoria” se pretenden tres cosas:

- Describir los temas abordados en la reunión (Cabe destacar que desde esta herramienta también se pueden ir formulando las Oportunidades de Mejora)
- Describir a los miembros de la reunión.
- Indicar las conclusiones y/o acuerdos.

A como se indicó en la sección 3.1.2, literal A, específicamente la parte relacionada con la Matriz de Riesgo, a continuación se contextualiza la ubicación en un Mapa de Riesgo Inherente, del Proceso en el cual se desarrollan una de las actividades principales que se hacen a través del Módulo de Caja.

Mapa de Riesgo – Riesgos Inherentes



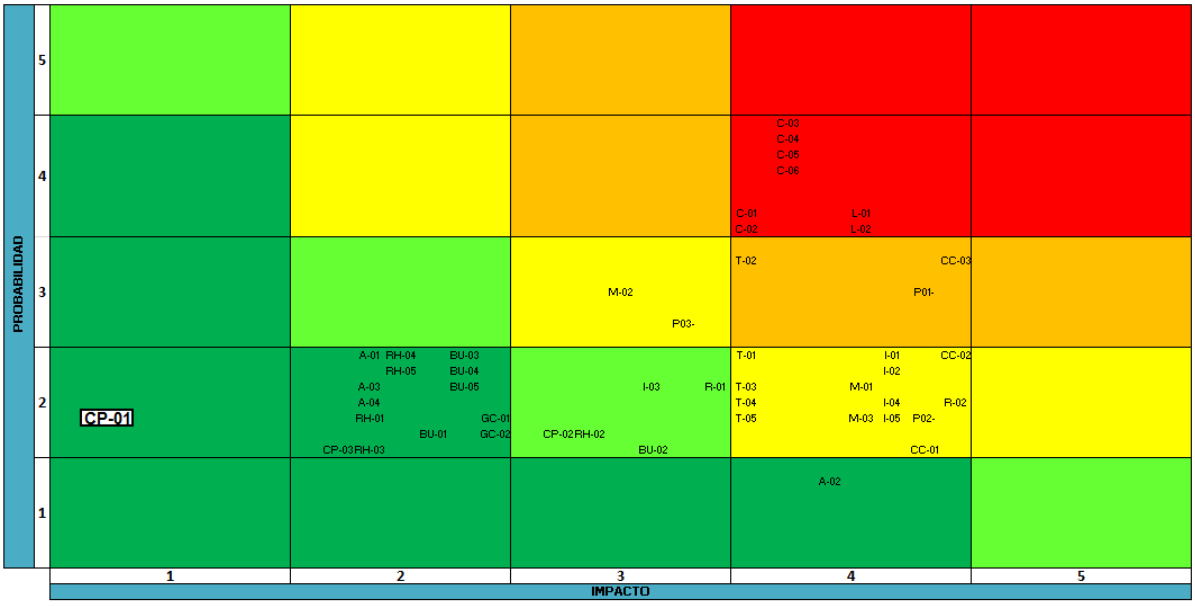
Para efecto de la contextualización, el código **CP-01(Recepción y retiro de depósitos)** resaltado en el Mapa de Riesgo corresponde a la ubicación con un valor de 16 puntos (Probabilidad ‘4’ X Impacto ‘4’) del proceso en el cual se involucran una

de las principales actividades que se hacen a través del módulo de caja a como se mencionó anteriormente (Recepción y entrega de efectivo – Deposito y Retiro).

Nota aclaratoria: Los demás códigos se omiten como parte de la delimitación al proceso de caja que se está contextualizando. Cabe destacar que una Matriz de Riesgo Inherente corresponde a la ubicación de los procesos de una institución en los valores del riesgo puro (sin controles) y es una herramienta que permite visualizar de forma gráfica en las escalas clasificadas por colores -Rojo (Riesgo Alto), Naranja (Riesgo Medio), Verde claro (Riesgo Bajo) y Verde oscuro (Riesgo muy bajo)-

Una vez que se diseñan, implementan y valoran los controles, se grafica un segundo Mapa de Riesgo, esta vez denominado Mapa de Riesgo - Residual, a continuación se indica la ubicación del proceso CP-01 con la aplicación de controles, en el cual como ejemplo se ubica en el cuadrante (2 X 1).

Mapa de Riesgo-Residual



4.2. Contextualización de la etapa de Ejecución.

A. Desarrollando el procedimiento de auditoría (S/ Programa de Auditoria)

Los procedimientos de auditoría deben desarrollarse de conformidad con el objetivo definido durante la planeación y aprobación del programa de Auditoría.

Cuando estos no son apropiados, el auditor deberá desarrollar el procedimiento en adendas al programa de trabajo, mismos que deben ser justificados y documentados en los papales de trabajo o Pts.

Es por ende que en concordancia con el desarrollo del procedimiento según el programa de Auditoría, retomamos el programa definido en el Items "Elaboración del Programa de Auditoría" con el fin de ejemplificar y/o contextualizar el desarrollo del mismo.

1. **Objetivo de Auditoria 1:** Verificar la efectividad del proceso que se efectúa en el cierre del Módulo de Caja.

   En este objetivo según el programa de Auditoría se definieron cuatro (4) procedimientos específicos para logra el objetivo, por consiguiente:

- El Auditor de Sistemas puede utilizar un formato de entrevistas que considere el adecuado para ir reafirmando la información más relevante del proceso de cierre documentada muy probablemente dentro del entendimiento del proceso. Nota aclaratoria: En cada desarrollo del procedimiento se pueden ir identificando oportunidades de mejoras las cuales serán abordadas en la Sección "Seguimiento a Oportunidades de Mejora".

- Para la verificación de la existencia de “Bitácoras de Cierre”, el Auditor de Sistemas debe identificar las principales tablas en las cuales se alojan todos los eventos que se registran en el cierre del Módulo estas pueden ser conocidas mediante la “herramienta de entrevista” con el Analista encargado del desarrollo del módulo.

- El análisis del código fuente es de vital importancia para entender a profundidad el funcionamiento del cierre del sistema es importante destacar que la revisión del mismo debe estar sujeta del área y la obtención del código fuente que se tiene en ambiente de producción puede obtenerse de diversas formas:

  - Solicitud formal del código fuente a la Gerencia de Tecnología
  - Solicitud de acceso al repositorio de códigos fuentes o control de versiones o VCS (Version Control System) en poder de la Gerencia de Tecnología; en esta sección existen diversos programas especializados para el alojamiento de los mismos, entre ellos se pueden mencionar Sourcesafe, ClearCase, CVS, Subversion, entre otros.

- Una vez identificado los procedimientos manuales y/o automáticos en el proceso de cierre del módulo, es importante reflejar el comportamiento histórico del cierre con el fin de ir cerrando las brechas que generan los posibles errores potenciales más sobresalientes.

Nota importante: Desde cualquier ejecución de los cuatro (4) procedimientos, se pueden identificar oportunidades de mejora, por ejemplo. Si en el proceso de revisión in situ se constata la no existencias de bitácoras se emite la primera oportunidad relacionada con su implementación, si en la revisión de los de las bitácora se comprueba que los errores se presentan reincidentemente en un proceso, se identifica la causa y se orienta la pronta corrección.

2. **Objetivo de Auditoría 2:** Verificar la efectividad de la aplicación de los tipos de cambio a través de la interfaz que tiene el Módulo Caja con el Módulo de Contabilidad en las operaciones de mesa de cambio.

   El desarrollo de este objetivo se puede basar en la ejecución de una prueba sustantiva, es decir el impacto que tiene la contabilización de las operaciones de mesa de cambio o bien en una prueba de control a nivel de los tipos de cambio que se asignan a cada operación.

- La verificación de una muestra de operaciones de mesas de cambio consiste en identificar todos los tipos de cambio que realiza la institución financiera.

  Ejemplo: Si un cliente llega a caja a cambiar dólares por moneda nacional, la institución bancaria está realizando una compra de lo contrario estaría realizando una venta, otro ejemplo puede ser una recarga electrónica a un celular, en la cual el cliente le entrega al cajero dólares, siguiente el ejemplo la institución también estaría realizando una compra a través de dos (2) operaciones, primero la mesa de cambio de compra y posteriormente la aplicación de la recarga electrónica.

  Sutilmente en esta sencilla operación intervienen varios factores que predisponen el expertis del auditor para verificar el adecuado funcionamiento del sistema en la conversión de la moneda; por ejemplo se puede realizar una prueba CAATs para constar que este correcto, pudiéndose utilizar herramientas como IDEA datos, ACL o bien procesadores de hojas de cálculos como Excel. Véase a continuación la ejecución de la prueba:

  La tabla 1, contiene el catálogo de Tipos de cambios parametrizados en el módulo de contabilidad por el personal asignado para esta actividad.

Tabla 1

Catálogo de Tipos de Cambio

Tipo de Cambio	**Compra**	**Venta**
Ventanilla	30.1000	30.2000
Especial	30.1700	30.1800
Súper Especial	30.1800	30.1900

Lo siguiente consistiría en validar para cada tipo de operación la correcta asignación del tipo de cambio. Por ejemplo, supongamos que se requiere validar la correcta aplicación del tipo de cambio para una venta que realiza el banco cuando el cliente se presenta a realizar una recarga electrónica a un celular, presentando efectivo en moneda extranjera (US$10), limitando el ejemplo a recalcular la operación a través de una hoja de procesamientos de datos (Excel).

La Tabla 2, contiene la aplicación del recalculo, sin embargo, quedaría pendiente de validar el recalculo contra el registro del sistema, mismo que será expresado en la **Tabla 3**

Tabla 2 Aplicación de la prueba			
Ref.	Detalle Operación	1	2
		Especial	Oficial
A	Tipo de Cambio	30.17	30.15
B	Monto (Cliente)	10.00	10.00
C	Valor Mesa de Cambio	301.70	301.50

Total Ingreso/Perdida (1C-2C)=	0.20

La siguiente tabla muestra el hipotético caso de una inadecuada parametrización utilizada en el código fuente para las operaciones de mesa de cambio.

Tabla 2
Aplicación de la prueba

Ref.	Detalle Operación	1	2
		Especial	Oficial
A	Tipo de Cambio	30.18	30.15
B	Monto (Cliente)	10.00	10.00
C	Valor Mesa de Cambio	301.80	301.50
Total Ingreso/Perdida (1C-2C)=		0.30	

En la validación de asignación de tipo de cálculo según los registros del módulo de caja vs contabilidad se observa un ingreso mayor al recalculo efectuado en la **tabla 2,** el cual corresponde según verificación en el código fuente de que el analista programó erróneamente la venta como que la institución financiera estuviera comprando. Dando continuidad al caso hipotético se deben de identificar todas las operaciones realizadas en el periodo para realizar los ajustes correspondientes en la contabilidad.

En esta fase se puede emitir una oportunidad de mejora relacionada con un proceso de revisión en la asignación de los tipos de cambios que se parametrizan en el sistema a través de código fuente o bien manejar un catálogo a nivel de forms (pantallas) para que se puedan ingresar y que a la vez sean autorizados por un tercero.

3. **Objetivo de Auditoría 3:** Verificar la adecuada segregación de funciones del personal encargado en efectuar las autorizaciones de operaciones de los cajeros.

   La verificación de segregación de funciones puede ser en cada auditoria de sistemas una revisión cajonera debido a la importancia que tienen la aplicación de las operaciones así como la aprobación.

   Para efecto de aplicar el procedimiento, se pueden utilizar herramientas tales como Script (códigos) de extracción desde la base de datos. **Nota:** En un sistema integrado y bien estructurado deberían de existir enrollamientos de pantallas por usuarios.

   Por lo cual se puede crear una Matriz sobre los cargos que tienen acceso a las pantallas que se están auditando; en este ejemplo a la opción de autorizaciones de ciertas operaciones que realizan los cajeros Vs los descriptores de puestos autorizados para estas operaciones. Los usuarios que estén por fuera de esta comparación requerirán de una inmediata depuración y eliminación de los accesos.

4.3. Contextualización de la etapa de Presentación de Resultados.

En el transcurso de una auditoría, los auditores designados a la revisión, mantendrán constante comunicación con los Auditados de la Institución Financiera, dándoles la oportunidad para presentar pruebas documentadas, así como información verbal pertinente respecto de los asuntos sometidos a examen; la comunicación de los resultados se la considera como una de las

última fase de la auditoría, sin embargo debe ser ejecutada durante todo el proceso.

Al finalizar los trabajos de auditoría en el campo, se dejará constancia documentada de que fue cumplida la comunicación de resultados en los términos previstos de acuerdo a la fase de planeación de la auditoria o bien por la normas en caso de aplicar y su ley en materia".

En esta fase se procede a la elaboración del informe, en donde el equipo de auditoría comunica a los funcionarios de la entidad auditada los resultados obtenidos durante todo el proceso de ejecución de la auditoría, **Véase en Anexo X** - Formato de Presentación de Resultados, conteniendo los principales elementos de acuerdo a mejores prácticas.

4.4. Contextualización de la etapa de Seguimiento a las Oportunidades de Mejora.

La Unidad de Auditoría Interna (UAI) deberá efectuar el seguimiento a las oportunidades de mejoras emitidas y comunicadas a la Gerencia encargada de implementarla (el seguimiento es continuo hasta que se implemente por completo).

Es importante destacar que para la superación de las oportunidades de mejora se deben de obtener y validar los soportes correspondientes que sean suficientes para atender integralmente la observación. Es importante destacar que el seguimiento se puede presentar ante el Comité de Auditoría y/o Junta Directiva con periodicidad mensual trimestral, etc. **Véase en Anexo XI** la propuesta de una matriz para efectuar el seguimiento a las oportunidades de mejoras.

BIBLIOGRAFÍA

Marcos de Referencias:

- COSO ERM
- COBIT Versión 4.0 y 5.0

Normativas y Regulaciones:

- Normas internacionales de Auditoría Interna (NIA) 2012.
- Norma sobre Gestión de Riesgo Tecnológico (Emitida por la Súper Intendencia de Bancos y Otras Instituciones Financieras SIBOIF).

Estándares Internacionales y/o mejores prácticas:

- ITIL (*Information Technology Infrastructure Library)* Version 3.

Páginas Web:

- http://ds5-andre-ortega-5a.host56.com/historia.html
- http://www.itil-officialsite.com/
- http://www.auditoriaadministrativa.com/concepto-auditoria-administrativa.htm

Libros:

- [Pressman, 2006] Roger S. Pressman, “Ingenieria del Software” 6ta edición, Editorial Concepcion Fernandez Madrid, 2006.
- [ISACA] ISACA.
- Paz, D. G. (2014). Metodología de la Investigación. Mexico: Grupo Editorial Patrica.
- Sampieri, R. H. (2014). Metodología de la Investigación. México DF: Mc Graw Hill.
- Manual preparación al examen CISA”, 22ª edición.

CONCLUSION

- La Ejecución de las Auditorias de Sistemas en particular la revisión de controles aplicativos es un complemento importante que permite dar aseguramiento a las instituciones financieras sobre los controles diseñados por el Negocio.

- Se determina que las principales fases de auditorías aplicadas en el Sistema Bancario corresponden a Fase de Planeación, Ejecución, Presentación de Resultados y Seguimiento a Oportunidades de Mejora.

- La metodología y o herramientas utilizadas por cada Institución Financiera es sigilosamente resguardada por cada una de ellas.

- La base teórica y/o lineamientos de las mejoras prácticas son la base para la ejecución de las auditorias, no obstante estas son tropocalizadas por cada institución financiera en el cual las herramientas también son diseñadas de conformidad con las necesidades de cada una de ellas.

RECOMENDACIONES

- Desarrollar nuevas metodologías a partir de la investigación realizada, de tal forma que el contenido de los instrumentos y pasos descritos en el presente estudio puedan ser rediseñados y mejorados a partir de los aportes que sean brindados por nuevos investigadores.

- Adaptar el contenido de cada uno de los instrumentos propuestos de acuerdo a las necesidades del departamento de auditoría interna de las instituciones financieras.

- Adecuar el contenido de la propuesta metodológica para que sea aplicable no sólo a la realización de auditorías de sistemas en instituciones financieras de primer piso, sino también para otro tipo de instituciones con otros giros de negocio (comercializadoras, empresas productoras de bienes y servicios, etc).

- Desarrollar una aplicación informática y/o adquirir una herramienta que permita sistematizar de una manera organizada y controlada la elaboración y seguimiento de cada uno de los instrumentos propuestos en las etapas de planeación, ejecución, presentación de resultados y seguimiento a las oportunidades de mejora.

ANEXOS

Anexo I - Encuesta sobre Auditoría de Sistemas

El propósito de la siguiente encuesta es conocer de manera general la forma de trabajo realizada por el área de auditoría interna en las instituciones bancarias de primer piso al momento de efectuar auditorías de sistemas informáticos.

NO SE SOLICITARA su nombre ni el de la institución bancaria a la que pertenece. Todas sus respuestas se manejarán de manera confidencial, solo aplicables al presente estudio.

1. Según su criterio, ¿cuáles son las fases que posee el proceso de una auditoría interna?

   _____

   _____

2. De las etapas que indicó en la respuesta anterior, ¿Cuál considera usted que es la etapa de la auditoría que conlleva mayor complejidad? ¿Por qué conlleva mayor complejidad?

   _____

   _____

3. ¿Considera usted que las fases del proceso de auditoría son Planeación, Ejecución, Presentación de Resultados y Mejora Continua?
   Si [ ] No [ ] Considero que pueden haber otras etapas [ ]

4. Si su respuesta anterior fue "Considero que puede haber otras etapas": Indique qué otras etapas deben de ser consideradas:

   _____

   _____

5. ¿Conoce cuál es la base bibliográfica, marco de trabajo o guía de mejores prácticas que defina que las fases de auditoría son Planeación, Ejecución, Presentación de Resultados y Seguimiento a las Oportunidades de Mejora?
   Si [ ] No [ ]

6. Si su respuesta anterior fue Si: Especifique cuál o cuáles son los marcos de trabajo y/o guías metodológicas que definen las fases de auditoría previamente mencionadas.
   _____
   _____

7. ¿Posee su unidad de auditoría interna una metodología y/o instrumentos definidos para la realización de la PLANEACION de la auditoría?
   Si [ ] No [ ] No sé [ ]

8. Si su respuesta a la pregunta anterior fue Si: ¿Cuál es el origen de dicha metodología? Puede seleccionar más de una opción:

   Está definida en los manuales operativos de auditoría interna [ ]
   Fue creada basándose en la experiencia del equipo de auditoría interna [ ]
   Fue creada basándose en un marco de trabajo en específico [ ]
   Otra [ ] _____

9. ¿Quién define los objetivos de la auditoría que le solicitan realizar? Puede seleccionar más de una opción:
   Alta Gerencia [ ]
   Comité de Auditoría [ ]
   Otros [ ] _____

10. Describa de manera general cuáles son las actividades que usted/su equipo de auditoría realiza al momento de tener que realizar la PLANEACION de una Auditoría de Sistemas.

    _____

    _____

11. ¿Cuenta con algún instrumento y/o procedimiento que le permita validar si las actividades que están planeando van a satisfacer los objetivos de la auditoría?

    Si [ ] No [ ]

12. La etapa de PLANEACION de auditoría como queda documentada/evidenciada?

    A través de formatos escritos y/o digitalizados (archivos de texto,word,excel) [ ]

    A través de un sistema [ ]

    Otros [ ] _____

13. Describa de manera breve como usted y/o su equipo de auditoría interna realiza la etapa de EJECUCION de una auditoría de sistemas.

    _____

    _____

14. ¿Cuenta con algún instrumento que le permita validar si las actividades que están realizando están apegadas a la planeación inicial?

    Si [ ] No [ ]

15. Las actividades que realiza en la fase de EJECUCION de la auditoría, ¿están basadas en algún marco de trabajo o metodología?
    Si [ ] No [ ]

16. Si su respuesta anterior fue Si: Especifique cuál es el marco de trabajo o metodología utilizado en la fase de EJECUCION de la auditoría.
    _____
    _____

17. Describa brevemente como realiza la fase de Presentación de Resultados.
    _____
    _____

18. Mencione cuales instrumentos utiliza para la Presentación de Resultados de Auditoría.
    _____
    _____

19. ¿Usted implementa la fase de Seguimiento de Oportunidades de Mejora?
    Si [ ] No [ ]

20. Si su respuesta anterior fue Si: Describa de manera breve como ejecuta el Seguimiento de Oportunidades de Mejora:
    _____

21. ¿Considera usted importante que las fases del proceso de auditoría se ejecuten de acuerdo a un marco de trabajo bien definido, basados en las mejores prácticas de auditoría de sistemas?
    Si [ ] No [ ]

Anexo II – Formato de Requerimientos Iniciales de Auditoría

Unidad de Auditoría Interna (UAI)
Centro Corporativo BancoABC
Teléf. XXXXXXXX
Managua, Nicaragua
http://www.bancoABC.com.ni

Banco ABC

<<Describir la fecha de inicio de la auditoria>> Managua, XX de Mes de 20XX

Sr. <<*Describir el Nombre del Gerente* >>
<<*Describir la Gerencia*>>
Su despacho

Estimado Sr. <<*Describir el Nombre del Gerente*>>:

De conformidad con las actividades programadas en nuestro plan anual de trabajo para el año 20XX, le informaos que hemos iniciando la revisión de <<*Describir la Actividad/Auditoría*>> con fecha de corte al XX de Mes de 20XX.

Para esta revisión ocasión acreditamos al siguiente Staff:

1. <<Describir el Nombre del Supervisor>>
2. <<Describir el Nombre del Auditor Encargado >>
3. <<Describir el Nombre del Auditor Encargado de Sistemas>>
4. [...]

Para desarrollar esta actividad requerimos de su Visto Bueno para iniciar el recorrido del proceso en las actividades que se realiza en el <<*Describir la Gerencia/Área*>> a revisar.

De ser necesario requerir información adicional, la estaremos solicitando con anticipación durante nuestra auditoria.

Atentamente,

<<*Describir el Nombre del Gerente de Auditoria /o Vice Gerente*>>
Gerente / Vice Gerente de Auditoría Interna.

C.c: Nombre del Funcionario (Asistente), Cargo del Funcionario
Pts (Papeles de Auditoría)

Anexo III - Formato de Ayuda Memoria

Unidad de Auditoría Interna (UAI)
Centro Corporativo BancoABC
Teléf. XXXXXXXX
Managua, Nicaragua
http://www.bancoABC.com.ni

Banco ABC

<<Describir la fecha de inicio de la auditoria>> Managua, XX de Mes de 20XX

AYUDA MEMORIA

<<Describir los asistentes de la reunión>>

Núm.	Nombre	Firma
1	*<<Describir el Nombre del Gerente >>, <<Describir el Cargo del Gerente >>*	
2	*<<Describir el Nombre del Vice Gerente >>, <<Describir el Cargo del Vice Gerente >>*	
4	*<<Describir el Nombre del Auditor Supervisor >>*	
5	*<<Describir el Nombre del Auditor Encargado>>*	

TEMA: *<<Describir el Tema Principal de la Reunión Inicial>>*

A- **Resumen** *<<Describir el Resumen de los temas abordados en la reunión >>*

Nota Aclaratoria: El resumen puede ser elaborado de la manera más sencilla, la cual les permita recalcar las partes más importantes de la Reunión, en ella se pueden indicar requerimientos adicionales del Gerente, se pueden considerar temas de riesgo y control, y brechas inidentificadas durante un proceso de análisis GAP.

B- **Conclusiones** / **Acuerdos** *<<Describir la conclusión y o acuerdos asumidos como parte de la Reunión >>*

Anexo IV – Análisis de Brecha o GAP

Unidad de Auditoría Interna (UAI)
Centro Corporativo BancoABC
Teléf. XXXXXXXX
Managua, Nicaragua
http://www.bancoABC.com.ni

Banco ABC

Proceso 1	Analisis de Brecha al Proceso XXX			Brecha/Aclaración/Comentarios
	Manual de Proceso 1	Manual de Proceso 2	Manual de Proceso ...	
Aclaracion: En esta sección se especifica el proceso al cual se hará en analisis de brecha. El proceso puede estar documentado o expresado verbalmente (ejecutado en la practica) por el dueño del proceso de forma verbal.	**Aclaracion:** Se pueude especificar la sección del Manual contra el cual se esta comparando la verificacion ya sea a traves de una prueba de observación y/o cualquier otra herramienta a utilizar	**Aclaracion:** Se pueude especificar la sección del Manual contra el cual se esta comparando la verificacion ya sea a traves de una prueba de observación y/o cualquier otra herramienta a utilizar		Se especifican las brechas a manera de comentarios y/o aclaraciones. En esta sección también se pueden ir señalando las oportunidades de mejora que resulten como parte de las brechas.

Preparado por: _____ Revisado por: _____ Autorizado por: _____

Anexo V – Matriz de Riesgo

Anexo VI – Formato de Plan de Trabajo de Auditoría

Unidad de Auditoría Interna (UAI)
Centro Corporativo BancoABC
Teléf.: XXXXXXXX
Managua, Nicaragua
http://www.bancoABC.com.ni

Banco ABC

<<Describir el Nombre de la Gerencia>>
<<Describir la fecha corte>>
Plan de Trabajo

1 → **Objetivo General**
<<Describir el Objetivo general de la revisión, este debe de coincidir con el objetivo de la presentación de los resultados emitidas en el informe de Auditoría>>

2 → **Objetivos Específicos**
<<Describir el o los Objetivos específicos de la revisión, también deben e coincidir con los objetivos a presentarse en el informe de Auditoría>>

3 → **Alcance de la auditoría**
<<Se describe el alcance de la revisión>> Véase a continuación un ejemplo definido de un alcance de revisión: "Transacciones registradas en el proceso XXX del sistema XXX en el período comprendido del 01 de enero de 20XX al 31 de diciembre de 20XX.

4 → **Limitaciones al alcance**
<<Se describen las posibles limitaciones de auditoría>> Ejemplo: "No tener acceso a los sistemas para extraer la información requerida"

5 → **Riesgos Asociados**
<<Se describen los riesgos asociados al proceso a revisar – Riesgos Reputacionales, de Cumplimiento, PLD, entre otros>>

6 → **Tipos de Pruebas a Utilizar**
<<Se definen las pruebas que se utilizaran>> Por ejemplo: "Pruebas CAAT'S, Pruebas de Cumplimiento, Pruebas Sustantivas"

Anexo VII – Programa de Auditoría

Unidad de Auditoría Interna (UAI)
Centro Corporativo BancoABC
Teléf. XXXXXXXX
Managua, Nicaragua
http://www.bancoABC.com.ni

Banco ABC

No	Objetivos de Auditoria	Procedimientos de Auditoria	REF PT´S	HECHO POR
1	Verificar la efectividad del proceso que se efectúa en el cierre del Módulo de Caja.	1.1- Efectuar visitas y entrevistas al personal encargado del cierre del módulo de caja; en ambiente de producción. 1.2- Verificar la existencia de bitácoras en el proceso de cierre 1.3- Analizar el código fuente utilizado en el proceso de cierre. 1.4- Efectuar Estadística de errores generados en el proceso de cierre.	***<<**Las referencias se utilizan para indicar de forma manual, la ubicación de los resultados obtenidos en la aplicación de los procedimientos de Auditoría.* ***Como punto y aparte las referencias en la actualidad se aplican de forma automática a través de la utilización de Software especializados en Auditorías>>***	***<<**Se indican las iniciales del Auditor que desarrollo el procedimientos con las distintas técnicas de Auditoria**>>***
2	Verificar la efectividad de la aplicación de los tipos de cambio a través de la interfaz que tiene el Módulo Caja con el Módulo de Contabilidad en las operaciones de mesa de cambio.	2.1- Verifique en una muestra de operaciones de mesa de cambio, la correcta aplicación de mesas de cambio, tanto para compra y venta de divisas. ***<<La ejemplificación de determinar el tamaño de la muestra se aborda en el Capitulo V, sección "Etapa de la Ejecución">>***		

3	Verificar la adecuada segregación de funciones del personal encargado en efectuar las autorizaciones de operaciones de los cajeros.	1- Realizar consultas a la base de datos. 2- Analizar los datos y comprobar la adecuada segregación de funciones		

Elaborado por: XXX Fecha:_____

Revisado por: XXX Fecha:_____

Autorizado por: XXX Fecha:_____

Anexo VIII – Check List

Unidad de Auditoría Interna (UAI)
Centro Corporativo BancoABC
Teléf. XXXXXXXX
Managua, Nicaragua
http://www.bancoABC.com.ni

Banco ABC

Núm.	Proceso	Atributos									Comentarios UAI
		1	2	3	4	5	6	7	8	9	
1	Proceso 1 de X	□	□	□	□	□	□	□	□	□	**<<***Se indican comentarios y/o observaciones de parte del Auditor de campo sobre cada atributo relevante de cual se identificaron incumplimientos y/o variaciones, desviaciones entre otros del proceso 1 de x***>>**
2	Proceso 2 de X	□	□	□	□	□	□	□	□	□	**<<***Se indican comentarios y/o observaciones de parte del Auditor de campo sobre cada atributo relevante de cual se identificaron incumplimientos y/o variaciones, desviaciones entre otros del proceso 2 de x***>>**

Leyenda <<en referencia al atributo>>	
1	<<Referencia a lo que corresponde el atributo 1>>.
…	<<Referencia a lo que corresponde el atributo…>>.
9	<<Referencia a lo que corresponde el atributo 9>>
…	<<Referencia a lo que corresponde el atributo…>>.

Lista de Valores	
Contiene	□
No contiene	□
No aplica	n/a

Elaborado por: XXX Fecha:_____
Revisado por: XXX Fecha:_____
Autorizado por: XXX Fecha:_____

Anexo IX – Herramienta de Selección de Muestra

Unidad de Auditoría Interna (UAI)
Centro Corporativo BancoABC
Teléf. XXXXXXXX
Managua, Nicaragua
http://www.bancoABC.com.ni

La formúla esta diseñada estadisticamente desde el punto de razonamiento, denominado inferencia estadística: En el se utilizan las caracteristicas de un subconjunto de la población (la muestra) para hacer afirmaciones (inferir) sobre la población en general.

Atributos

- n es el tamaño de la muestra;
- Z es el nivel de confianza;
- P es la variabilidad positiva;
- Q es la variabilidad negativa;
- E es la precisión o error.

Niveles de confianza

%	Z
80%	1.2816
85%	1.4395
90%	1.6449
95%	1.9600
99%	2.5758

Proporción de elementos que:			
Cumplen con los controles internos	**P=**	95%	
No cumplen con los C.I.	**Q=**	5%	
Nivel de confiabilidad	**Z=**	90%	1.6449
Error máximo permisible	**E=**	5%	
Tamaño de la Población			

CALCULO

Partiendo del supuesto que no se conoce el tamaño exacto de la población, pero con seguridad ésta se encuentra cerca a los diez millares

$$n = \frac{Z^2 p q}{E^2} = \frac{0.1285}{0.0025} =$$

Si se conoce la Población:

$$n = \frac{Z^2 p q N}{N E^2 + Z^2 p q} =$$

Realizado por:

Anexo X – Propuesta de Presentación de Informe

Unidad de Auditoría Interna (UAI)
Centro Corporativo BancoABC
Teléf. XXXXXXXX
Managua, Nicaragua
http://www.bancoABC.com.ni

Banco ABC

<< Se define la fecha>> Semejante al formato de una carta

<< Se indica a quien va dirigida la carta>>

<<Se indica una breve descripción del proceso revisado>>

I. OBJETIVOS ESPECIFICOS

<<Se expresan los Objetivos Específicos de la Revisión, deben de coincidir con la Sistematización, Programa y Plan de Trabajo>>.

II. ALCANCE

<<Se indica el alcance, el cual debe coincidir con el Plan de Trabajo>>

III. PROCEDIMIENTOS

<<Se expresan los procedimientos generales utilizados para desarrollar la auditoría>>

II. ALCANCE

<<Se indica el alcance, el cual debe coincidir con el Plan de Trabajo>>

III. PROCEDIMIENTOS

<<Se expresan los procedimientos generales utilizados para desarrollar la auditoría>>

IV. RESULTADOS

<<Se describen los resultados obtenidos por cada procedimiento desarrollado en el transcurso de la auditoria>>

V. CONCLUSIÓN

<<Se describe las conclusión de la revisión efectuada, estas deben ser consistentes con cada objetivo planteado en la sección de Objetivos Específicos o General>>

VI. OPORTUNIDADES DE MEJORAS

<<En caso de existir Oportunidades de Mejoras producto del resultado de la Auditoría, se detallan en esta sección >> Véase formato utilizado en la sección de "Ejecución"

Nota: El informe debe ser firmado por el Auditor General y también puede incluirse una sección de Anexos.

Anexo XI – Matriz de Seguimiento a Oportunidad de Mejoras